HP ProtectTools
Guia do Usuário

Conteúdo

1 Introdução à segurança

O software HP ProtectTools Security Manager fornece recursos de segurança que ajudam a proteger contra acesso não-autorizado ao computador, redes e dados confidenciais. Funções avançadas de segurança são fornecidas pelos seguintes módulos de software:

- Credential Manager for HP ProtectTools
- Drive Encryption for HP ProtectTools (somente em determinados modelos)
- Privacy Manager for HP ProtectTools (somente em determinados modelos)
- File Sanitizer for HP ProtectTools
- BIOS Configuration for HP ProtectTools
- Embedded Security for HP ProtectTools (somente em determinados modelos)
- Device Access Manager for HP ProtectTools (somente em determinados modelos)

Os módulos de software disponíveis para seu computador podem variar de acordo com o modelo. Por exemplo, o Embedded Security for HP ProtectTools está disponível somente em computadores que possuem o chip de segurança integrada TPM (Trusted Platform Module) instalado.

Os módulos de software do HP ProtectTools podem estar pré-instalados, pré-carregados ou disponíveis para download do Web site da HP. Visite http://www.hp.com para obter mais informações.

NOTA: As instruções neste guia foram escritas considerando-se que os módulos do software HP ProtectTools aplicáveis já estão instalados.

Recursos do HP ProtectTools

A tabela a seguir detalha os principais recursos dos módulos do HP ProtectTools:

Módulo	Principais recursos
Credential Manager for HP ProtectTools	• O Credential Manager atua como um cofre de senhas pessoal, otimizando o processo de login com o recurso Single Sign On (Login Único), que recorda e aplica as credenciais do usuário automaticamente. • O recurso Single Sign On também oferece proteção adicional, pois exige uma combinação de diferentes tecnologias de segurança, como Java™ Card e biometria, para efetuar a autenticação de usuários. • O armazenamento de senhas é protegido por meio de criptografia de software e essa proteção pode ser aprimorada com o uso de um chip de segurança integrado TPM e/ou da autenticação via dispositivos de segurança, como Java Cards ou dados biométricos.
Drive Encryption for HP ProtectTools (somente em determinados modelos)	• O Drive Encryption fornece criptografia completa para uma unidade de disco inteira ("full-volume"). • O Drive Encryption força uma autenticação durante a pré-inicialização para que os dados sejam descriptografados e possam ser acessados.
Privacy Manager for HP ProtectTools (somente em determinados modelos)	• O Privacy Manager utiliza técnicas de login avançadas para verificar a origem, integridade e segurança da comunicação ao utilizar e-mail, documentos do Microsoft® Office ou troca de mensagens instantâneas.
File Sanitizer for HP ProtectTools	• O File Sanitizer permite fragmentar com segurança ativos digitais (informações confidenciais que incluem arquivos de aplicativos, dados de histórico ou relacionados à Web, ou outros dados confidenciais) do computador e periodicamente limpar sua unidade de disco rígido.
BIOS Configuration for HP ProtectTools	• O BIOS Configuration fornece acesso ao gerenciamento de senhas de inicialização de administradores e usuários. • O BIOS Configuration oferece uma alternativa em relação ao utilitário de configuração do BIOS na pré-inicialização conhecido como utilitário de configuração do computador (Computer Setup). • A ativação pelo BIOS Configuration do suporte ao DriveLock Automático, o qual é aprimorado com o chip de segurança integrado, ajuda a proteger unidades de disco rígido contra acesso não-autorizado, mesmo quando a unidade é removida do sistema, sem exigir que o usuário memorize senhas adicionais além da senha de usuário do chip de segurança integrado.

Módulo	Principais recursos
Embedded Security for HP ProtectTools (somente em determinados modelos)	• O Embedded Security utiliza um chip de segurança integrada TPM (Trusted Platform Module) para ajudar a proteger contra o acesso não-autorizado a dados confidenciais do usuário ou credenciais armazenados localmente no computador. • O Embedded Security permite a criação de uma unidade pessoal protegida (PSD), útil para a proteção de informações de arquivos e pastas de usuários. • O Embedded Security fornece suporte a aplicativos de terceiros (como Microsoft Outlook e Internet Explorer) para operações com certificados digitais protegidas.
Device Access Manager for HP ProtectTools (somente em determinados modelos)	• O Device Access Manager permite aos gerentes de TI controlar o acesso aos dispositivos com base em perfis de usuário. • O Device Access Manager evita que usuários não-autorizados removam dados utilizando mídia de armazenamento externo e introduzam vírus no sistema provenientes de mídia externa. • O administrador pode desativar o acesso a dispositivos graváveis para determinados indivíduos ou grupos de usuários.

Acesso ao HP ProtectTools Security

Para acessar o HP ProtectTools Security Manager a partir do Painel de Controle do Windows®:

1. No Windows Vista®, clique em **Iniciar** e, em seguida, clique em **HP ProtectTools Security Manager for Administrators**.

   – ou –

   No Windows XP, clique em **Iniciar**, **Todos os programas** e, em seguida, clique em **HP ProtectTools Security Manager**.

   NOTA: Se você não for um administrador do HP ProtectTools, poderá executar o HP ProtectTools no modo não-administrador para exibir informações, mas não poderá fazer alterações.

2. No painel esquerdo, clique em **HP ProtectTools** e, em seguida, clique em **Getting Started** (Passos iniciais).

3. Clique no botão **Security Manager Setup** (Configuração do Security Manager), diretamente abaixo do ícone de escudo do HP ProtectTools, para iniciar o assistente do Security Manager.

   A seguinte página é exibida:

- O assistente guia os administradores do sistema operacional Windows através da configuração dos níveis de segurança e dos métodos de login de segurança usados em um ambiente de pré-inicialização, no Credential Manager e no Drive Encryption.
- Os usuários também utilizam o assistente de instalação para configurar seus métodos de login de segurança.

NOTA: Para acessar cada módulo do HP ProtectTools para configurar recursos mais poderosos, clique no ícone do módulo.

NOTA: Após a configuração do módulo Credential Manager, também será possível abrir HP ProtectTools efetuando login diretamente no Credential Manager a partir da tela de login do Windows. Para obter mais informações, consulte "Efetuar login no Windows com Credential Manager na página 17".

Alcançando os principais objetivos de segurança

Os módulos do HP ProtectTools podem funcionar em conjunto para fornecer soluções para diversos problemas de segurança, incluindo os principais objetivos de segurança a seguir:

- Proteção contra roubo direcionado
- Restrição de acesso a dados confidenciais
- Prevenção contra acesso não-autorizado a partir de locais internos ou externos
- Criação de políticas de senhas fortes
- Tratar de questões de segurança regulamentares

Proteção contra roubo direcionado

Um exemplo deste tipo de incidente poderia ser o roubo direcionado de um computador contendo dados confidenciais e informações de clientes em um ponto de controle de segurança de um aeroporto. Os seguintes recursos ajudam a proteger contra roubo direcionado:

- O recurso de autenticação na pré-inicialização, se ativado, ajuda a evitar o acesso ao sistema operacional. Consulte os seguintes procedimentos:
  - Credential Manager
  - Embedded Security
  - Drive Encryption
- O DriveLock ajuda a garantir que os dados não possam ser acessados mesmo se a unidade de disco rígido for removida e instalada em um sistema desprotegido.
- O recurso Personal Secure Drive, fornecido pelo módulo Embedded Security for HP ProtectTools, criptografa dados confidenciais para ajudar a garantir que não possam ser acessados sem autenticação. Consulte os seguintes procedimentos:
  - Embedded Security “Procedimentos de configuração na página 76”
  - “Utilização de Personal Secure Drive (PSD) na página 79”

Restrição de acesso a dados sensíveis

Suponha que um auditor contratado esteja trabalhando localmente em uma empresa e tenha obtido acesso ao computador para revisar dados financeiros confidenciais; não se deseja que o auditor possa imprimir os arquivos ou salvá-los em um dispositivo gravável, como um CD. Os seguintes recursos ajudam a restringir o acesso aos dados:

- O Device Access Manager for HP ProtectTools permite aos gerentes de TI restringir o acesso a dispositivos graváveis de modo que informações confidenciais não possam ser impressas ou copiadas da unidade de disco rígido para uma mídia removível. Consulte “Configuração de classe de dispositivo (avançado) na página 87”.
- O DriveLock ajuda a garantir que os dados não possam ser acessados mesmo se a unidade de disco rígido for removida e instalada em um sistema desprotegido.

Prevenção contra acesso não-autorizado a partir de locais internos ou externos

O acesso não autorizado a um PC comercial desprotegido representa um risco bastante tangível aos recursos de rede corporativos, como informações de serviços financeiros, de um executivo ou da equipe de P&D, e informações confidenciais como registros de patente ou registros financeiros pessoais. Os seguintes recursos ajudam a evitar o acesso não-autorizado:

- O recurso de autenticação na pré-inicialização, se ativado, ajuda a evitar o acesso ao sistema operacional. Consulte os seguintes procedimentos:
  - Credential Manager
  - Embedded Security
  - Drive Encryption
- O Embedded Security for HP ProtectTools ajuda a proteger dados confidenciais do usuário ou credenciais armazenados localmente no computador utilizando os seguintes procedimentos:
  - Embedded Security “Procedimentos de configuração na página 76”
  - “Utilização de Personal Secure Drive (PSD) na página 79”
- Através dos procedimentos a seguir, o Credential Manager for HP ProtectTools ajuda a garantir que um usuário não-autorizado não possa obter senhas ou acessar aplicativos protegidos por senha:
  - Credential Manager “Procedimentos de configuração na página 12”
  - “Utilização do recurso Single Sign On na página 18”
- O Device Access Manager for HP ProtectTools permite aos gerentes de TI restringirem o acesso a dispositivos graváveis de modo que informações confidenciais não possam ser copiadas da unidade de disco rígido. Consulte “Configuração simples na página 86”.
- O recurso Personal Secure Drive criptografa dados confidenciais para ajudar a garantir que não possam ser acessados sem autenticação e utiliza os seguintes procedimentos:
  - Embedded Security “Procedimentos de configuração na página 76”
  - “Utilização de Personal Secure Drive (PSD) na página 79”

Criação de políticas de senhas fortes

Se entrar em efeito uma ordem exigindo o uso de uma política de senha forte para diversos aplicativos baseados na web e bancos de dados, o Credential Manager for HP ProtectTools fornece um repositório de senhas protegido e o conveniente recurso Single Sign On utilizando os seguintes procedimentos:

- Credential Manager - “Procedimentos de configuração na página 12”
- “Utilização do recurso Single Sign On na página 18”

Para oferecer uma maior segurança, o Embedded Security for HP ProtectTools então protege esse repositório de nomes de usuário e senhas. Isso permite que os usuários mantenham diversas senhas fortes sem precisar anotá-las ou memorizá-las. Consulte Embedded Security - “Procedimentos de configuração na página 76”.

Elementos adicionais de segurança

Atribuição de perfis de segurança

No gerenciamento da segurança de computador (principalmente em grandes organizações), uma prática importante é dividir as responsabilidades e os direitos entre vários tipos de administradores e usuários.

NOTA: Em uma organização pequena ou para uso individual, esses perfis podem ser mantidos pela mesma pessoa.

Para o HP ProtectTools, as obrigações e os privilégios da segurança podem ser divididos nas seguintes funções:

- Diretor de segurança - Define o nível de segurança para a empresa ou rede e determina os recursos de segurança a implementar, como Java™ Cards, leitores biométricos ou tokens USB.

  NOTA: Diversos recursos do HP ProtectTools podem ser personalizados pelo responsável pela segurança em conjunto com a HP. Para obter mais informações, consulte o Web site da HP em http://www.hp.com.

- Administrador de TI – Aplica e gerencia os recursos de segurança definidos pelo diretor de segurança. Pode também ativar e desativar alguns recursos. Por exemplo, se o responsável pela segurança tiver decidido implementar Java Cards, o administrador de TI pode ativar o modo de segurança do BIOS por Java Card.
- Usuário - Utiliza os recursos de segurança. Por exemplo, se o responsável pela segurança e o administrador de TI tiverem ativado Java Cards para o sistema, o usuário pode definir o PIN do Java Card e usar o cartão para autenticação.

Gerenciamento de senhas do HP ProtectTools

A maioria dos recursos do HP ProtectTools Security Manager são protegidos por senhas. A tabela a seguir lista as senhas mais usadas, o módulo de software em que a senha é definida e a função da senha.

As senhas definidas e usadas somente por administradores de TI também são indicadas nesta tabela. Todas as outras senhas podem ser definidas por usuários ou administradores comuns.

Senha do HP ProtectTools	Definida neste módulo do HP ProtectTools	Função
Senha de login do Credential Manager	Credential Manager	Esta senha oferece duas opções: • Pode ser usada em um login separado para acessar o Credential Manager após o login no Windows. • Pode ser usada em lugar do processo de login do Windows, permitindo acessar simultaneamente o Windows e Credential Manager.
Senha de arquivo de recuperação do Credential Manager	Credential Manager, pelo administrador de TI	Protege o acesso ao arquivo de recuperação do Credential Manager.
Senha de chave de usuário básico	Embedded Security	Usada para acessar os recursos de Embedded Security, como e-mail protegido e criptografia de arquivos e pastas. Quando

Senha do HP ProtectTools	Definida neste módulo do HP ProtectTools	Função
NOTA: Também conhecida como Senha de Embedded Security		usada para autenticação na inicialização, protege também o acesso ao conteúdo do computador quando este é ligado, reiniciado ou sair da hibernação.
Senha de token de recuperação de emergência **NOTA:** Também conhecida como Senha de chave de token de recuperação de emergência	Embedded Security, pelo administrador de TI	Protege o acesso ao Token de recuperação de emergência, que é um arquivo de backup para o chip de segurança integrada.
Senha de proprietário	Embedded Security, pelo administrador de TI	Protege o sistema e o chip TPM de acesso não-autorizado a todas as funções do proprietário de Embedded Security.
PIN do Java™ card	Java Card Security	Protege o acesso ao conteúdo do Java Card e autentica usuários do Java card. Ao ser usado para autenticação na inicialização, o PIN do Java Card também protege o acesso ao utilitário de configuração do computador e ao conteúdo do computador. Autentica usuários do Drive Encryption, se o token de Java Card estiver selecionado.
Senha do Utilitário de configuração **NOTA:** Também conhecida como senha de administrador do BIOS, de Configuração f10 ou configuração de segurança	BIOS Configuration, pelo administrador de TI	Protege o acesso ao utilitário de configuração do computador.
Senha de inicialização	BIOS Configuration	Protege o acesso ao conteúdo do computador quando este for ligado, reiniciado ou sair da hibernação.
Senha de login do Windows	Painel de controle do Windows	Pode ser usada no login manual ou salva no Java Card.

Criação de uma senha de segurança

Ao criar senhas, é preciso primeiro seguir as especificações definidas pelo programa. Em geral, entretanto, considere as instruções a seguir para ajudar a criar senhas fortes e reduzir as chances de sua senha ser comprometida:

- Use senhas com mais de 6 caracteres, de preferência mais de 8.
- Misture letras maiúsculas e minúsculas na senha.
- Sempre que possível, misture caracteres alfanuméricos e inclua caracteres especiais e sinais de pontuação.
- Substitua caracteres especiais ou números por letras em uma palavra-chave. Por exemplo, use o número 1 para substituir as letras I ou L.
- Combine palavras de 2 ou mais idiomas.
- Divide uma palavra ou frase com números ou caracteres especiais no meio, por exemplo, “Mary2-2Cat45.”
- Não use uma senha que poderia aparecer em um dicionário.
- Não use seu nome como senha, ou qualquer outra informação pessoal, como data de aniversário, nomes de animais de estimação, ou nome de solteira da mãe, mesmo se soletrar invertido.
- Altere as senhas regularmente. É possível mudar uma senha apenas adicionando dois caracteres.
- Se escrever sua senha, não a guarde em um local bastante visível, muito perto do computador.
- Não guarde a senha em um arquivo, como um e-mail, no computador.
- Não compartilhe contas nem informe sua senha a qualquer pessoa.

Backup e restauração de credenciais do HP ProtectTools

Para fazer backup e restaurar credenciais de todos os módulos aceitos pelo HP ProtectTools, consulte o seguinte:

Backup de credenciais e configurações

É possível fazer backup de credenciais das seguintes maneiras:

- Use o Drive Encryption for HP ProtectTools para selecionar e fazer backup de credenciais do HP ProtectTools.

  Também é possível registrar-se no Serviço de recuperação de chave do Drive Encryption para armazenar uma cópia backup de sua chave de criptografia, que permitirá a você acessar o computador caso esqueça sua senha e não tenha acesso a seu backup local.

  NOTA: Você deve estar conectado à Internet e ter um endereço de e-mail válido para registrar e recuperar sua senha através desse serviço.

- Use o Embedded Security for HP ProtectTools para fazer backup de credenciais do HP ProtectTools.

2 Credential Manager for HP ProtectTools

O Credential Manager for ProtectTools protege contra o acesso não-autorizado a seu computador utilizando os seguintes recursos de segurança:

- Alternativas para senhas no início de sessão do Windows, como a utilização de um Java Card ou leitor biométrico para efetuar login no Windows. Para obter mais informações, consulte “Credenciais registradas na página 12”.
- O recurso Single Sign On, que recorda automaticamente as senhas de web sites, aplicativos e recursos de rede protegidos.
- Suporte para dispositivos de segurança opcionais, como Java Cards e leitores biométricos.
- Suporte a configurações de segurança adicionais, como requisição de autenticação com um dispositivo de segurança opcional para desbloquear o computador.

Procedimentos de configuração

Login no Credential Manager

Dependendo da configuração, você pode efetuar login no Credential Manager de uma das seguintes maneiras:

- Ícone do HP ProtectTools Security Manager na área de notificação
- No Windows Vista®, clique em **Iniciar** e, em seguida, clique em **HP ProtectTools Security Manager for Administrators**.
- No Windows XP, clique em **Iniciar** e, em seguida, clique em **HP ProtectTools Security Manager**.

NOTA: No Windows Vista, é necessário iniciar o HP ProtectTools Security Manager for Administrators para fazer alterações.

Após fazer login no Credential Manager, você poderá registrar credenciais adicionais, como uma impressão digital ou um Java Card. Para obter mais informações, consulte "Credenciais registradas na página 12".

No próximo login, é possível selecionar a regra de login e usar qualquer combinação de credenciais registradas.

Utilização do assistente de login do Credential Manager

Para efetuar login no Credential Manager utilizando o assistente de login do Credential Manager, use as seguintes etapas:

1. Abra o assistente de login do Credential Manager de uma das seguintes maneiras:
   - A partir da tela de login do Windows
   - A partir da área de notificação, clicando duas vezes no ícone **HP ProtectTools Security Manager**
   - A partir da página "Credential Manager" do HP ProtectTools Security Manager, clicando no link **Log On** (Logon) no canto superior direito da janela.
2. Siga as instruções apresentadas na tela para fazer login no Credential Manager.

Credenciais registradas

Você pode utilizar a página "Minha identidade" para registrar seus vários métodos de autenticação ou credenciais. Após o registro, é possível usar esses métodos para efetuar login no Credential Manager.

Registro de impressões digitais

O leitor de impressão digital permite efetuar o login no Windows usando sua impressão digital para autenticação, ao invés de utilizar uma senha do Windows.

Configuração do leitor de impressão digital

1. No HP ProtectTools Security Manager, clique em **Credential Manager** no painel esquerdo.
2. Clique em **My Identity** (Minha identidade) e, em seguida, clique em **Register Fingerprints** (Registrar Impressões Digitais).
3. Siga as instruções apresentadas na tela para concluir o registro de suas impressões digitais e configurar o leitor de impressão digital.
4. Para configurar o leitor de impressões digitais para um usuário do Windows diferente, efetue o login no Windows como esse usuário e repita as etapas listadas acima.

Utilizar sua impressão digital registrada para efetuar login no Windows

1. Imediatamente após ter registrado suas impressões digitais, reinicie o Windows.
2. Na tela Bem-vindo ao Windows, deslize qualquer de seus dedos registrados para efetuar login no Windows.

Registro de um Smart Card ou Token

O smart card é um cartão de plástico do tamanho de um cartão de crédito que possui um microchip incorporado e pode ser carregado com informações. Os smart cards fornecem proteção de informações e autenticação para usuários individuais. O login em uma rede com um smart card pode oferecer um método forte de autenticação quando utiliza identificação baseada em criptografia e prova de posse na autenticação de um usuário para um domínio.

Um token USB é simplesmente um smart card em um tamanho diferente. Em vez de implementar o smart chip em uma plataforma de cartão de plástico, o smart chip é inserido em um token plástico, também conhecido como chave USB. A principal diferença entre um smart card e um token está na interface de acesso. Um cartão requer um leitor, enquanto um token pode ser conectado diretamente a qualquer porta USB. Não há diferença na funcionalidade principal de armazenamento e fornecimento de credenciais.

Um token USB é usado para autenticação forte. Ele fornece segurança aprimorada e garante o acesso seguro às informações.

NOTA: Você deve ter um leitor de cartão configurado para este procedimento. Se você não tiver um leitor instalado, você pode registrar um token virtual como descrito em “Criar um token virtual na página 15.”

1. No HP ProtectTools Security Manager, clique em **Credential Manager** no painel esquerdo.
2. Clique em **My Identity** (Minha identidade) e, em seguida, clique em **Register Smart Card or Token** (Registro de Smart Card ou Token).
3. Na caixa de diálogo **Device Type** (Tipo de dispositivo), clique no tipo de dispositivo desejado e, em seguida, clique em **Next** (Avançar).
4. Se um smart card ou token USB foi selecionado como o tipo de dispositivo, verifique se o smart card foi inserido ou se o token foi conectado a uma porta USB.

   NOTA: Se o smart card não estiver inserido ou o token USB não estiver conectado, o botão Next (Avançar) fica desativado na caixa de diálogo Select Token (Selecionar token).

5. Na caixa de diálogo Device Type (Tipo de dispositivo), selecione **Next** (Avançar).

A caixa de diálogo Token Properties (Propriedades do token) é exibida.

6. Insira o PIN de usuário, selecione **Register smart card or token for authentication** (Registrar smart card ou token para autenticação) e, em seguida, clique em **Concluir**.

Registrar outras credenciais

1. No HP ProtectTools Security Manager, clique em **Credential Manager**.
2. Clique em **My Identity** (Minha identidade) e, em seguida, clique em **Register Credentials** (Registro de credenciais).

   O Credential Manager Registration Wizard (Assistente de Registro do Credential Manager) é exibido.
3. Siga as instruções na tela.

Tarefas básicas

Todos os usuários acessam a página “Minha identidade” no Credential Manager. A partir da página “Minha identidade” você pode desempenhar as seguintes tarefas:

- Alterar a senha de login do Windows
- Alterar o PIN de um token
- Bloquear uma estação de trabalho

NOTA: Esta opção está disponível somente se a solicitação de login clássica de Credential Manager estiver ativada. Consulte “Exemplo 1—Utilizando a página “Configuração avançada” para permitir o login do Windows a partir do Credential Manager na página 25”.

Criar um token virtual

Um token virtual funciona de forma muito semelhante a um Java Card ou Token USB. O token é salvo no disco rígido do computador ou no registro do Windows. Ao efetuar login com um token virtual, será solicitado um PIN de usuário para completar a autenticação.

Para criar um novo token virtual:

1. No HP ProtectTools Security Manager, clique em **Credential Manager** no painel esquerdo.
2. Clique em **My Identity** (Minha identidade) e, em seguida, clique em **Register Smart Card or Token** (Registro de Smart Card ou Token).
3. Na caixa de diálogo **Device Type** (Tipo de dispositivo), clique em **Virtual Token** (Token virtual) e, em seguida, clique em **Next** (Avançar).
4. Especifique o nome e o local do token e clique em **Next** (Avançar).

   Um novo token virtual pode ser armazenado em um arquivo ou no banco de dados de registro do Windows.
5. Na caixa de diálogo Token Properties (Propriedades do token), especifique o PIN Mestre e o PIN de Usuário para o token virtual recém-criado, selecione **Register smart card or token for authentication** (Registrar smart card ou token para autenticação) e clique em **Finish** (Concluir).

Alterar senha de login do Windows

1. No HP ProtectTools Security Manager, clique em **Credential Manager** no painel esquerdo.
2. Clique em **My Identity** (Minha identidade) e, em seguida, clique em **Change Windows Password** (Alterar senha do Windows).
3. Digite sua senha antiga na caixa **Senha antiga**.
4. Digite sua nova senha nas caixas **Nova senha** e **Confirmar senha**.
5. Clique em **Concluir**.

Alteração de um PIN de token

1. No HP ProtectTools Security Manager, clique em **Credential Manager** no painel esquerdo.
2. Clique em **My Identity** (Minha identidade) e, em seguida, clique em **Change Token PIN** (Alterar PIN de Token).
3. Na caixa de diálogo Device Type (Tipo de dispositivo), clique no tipo de dispositivo desejado e, em seguida, clique em **Next** (Avançar).
4. Selecione o token para o qual deseja alterar o PIN e, em seguida, clique em **Avançar**.
5. Siga as instruções apresentadas na tela para concluir a alteração do PIN.

NOTA: Se você inserir o PIN incorreto para o token várias vezes em seqüência, o token será bloqueado. Você não poderá usar esse token até que ele seja desbloqueado.

Bloqueio do computador (estação de trabalho)

Este recurso está disponível se você efetuar o login no Windows utilizando Credential Manager. Para proteger o computador quando se ausentar de sua mesa, utilize o recurso de bloqueio de workstation. Isso impede que usuários não autorizados tenham acesso a seu computador. Somente você e membros do grupo de administradores em seu computador podem desbloqueá-lo.

NOTA: Esta opção está disponível somente se a solicitação de login clássica de Credential Manager estiver ativada. Consulte “Exemplo 1—Utilizando a página “Configuração avançada” para permitir o login do Windows a partir do Credential Manager na página 25”.

Para aumentar a segurança, é possível configurar o recurso Lock Workstation (Bloquear estação de trabalho) para exigir um Java Card, leitor biométrico ou token para desbloquear o computador. Para obter mais informações, consulte “Definição de configurações do Credential Manager na página 25”.

1. No HP ProtectTools Security Manager, clique em **Credential Manager** no painel esquerdo.
2. Clique em **My Identity** (Minha identidade).
3. Clique em **Lock Workstation** (Bloquear estação de trabalho) para bloquear o computador imediatamente.

   É necessário usar uma senha do Windows ou o assistente Credential Manager Logon Wizard para desbloquear o computador.

Utilização do logon do Windows

Você pode utilizar o Credential Manager para efetuar login no Windows, no computador local ou em um domínio de rede. Quando você efetuar logon no Credential Manager pela primeira vez, o sistema adicionará automaticamente sua conta de usuário local do Windows como a conta para o serviço de logon do Windows.

Efetuar login no Windows com Credential Manager

Você pode usar o Credential Manager para efetuar logon para uma conta de rede Windows ou local.

1. Se você tiver registrado sua impressão digital para efetuar logon no Windows, deslize seu dedo para efetuar logon.
2. No Windows XP, se você não registrou sua impressão digital para efetuar login no Windows, clique no ícone de teclado no canto superior esquerdo da tela ao lado do ícone de impressão digital. O Credential Manager Logon Wizard (Assistente de Login do Credential Manager) é exibido.

   No Windows Vista, se você não registrou sua impressão digital para efetuar login no Windows, clique no ícone **Credential Manager** na tela de login. O Credential Manager Logon Wizard (Assistente de Login do Credential Manager) é exibido.
3. Clique na seta **Nome do usuário** e, em seguida, clique em seu nome.
4. Digite sua senha na caixa **Senha**, em seguida clique em **Avançar**.

5. Selecione **More** (Mais) e, em seguida, clique em **Wizard Options** (Opções de assistente).
   a. Se desejar que este seja o nome de usuário padrão na próxima vez em que efetuar login no computador, marque a caixa de seleção **Usar nome do último usuário no próximo logon**.
   b. Se desejar esta política de logon como método padrão, marque a caixa de seleção **Usar última política no próximo logon**.
6. Siga as instruções na tela. Se as informações de autenticação estiverem corretas, o login será efetuado na conta do Windows e no Credential Manager.

Utilização do recurso Single Sign On

O Credential Manager possui um recurso Single Sign On que armazena nomes e senhas de usuário para diversos programas do Windows e Internet, e insere automaticamente as credenciais de login quando um programa registrado é acessado.

NOTA: Segurança e privacidade são recursos importantes do Recurso Single Sign On. Todas as credenciais são criptografadas e estão disponíveis somente após o login bem-sucedido no.

NOTA: É possível também configurar o recurso Single Sign On para validar suas credenciais de autenticação com um Java Card, um leitor de impressão digital ou um token antes de efetuar login em um site ou programa protegido. Isso é particularmente útil ao efetuar login em programas ou web sites que contenham informações pessoais, como números de conta bancária. Para obter mais informações, consulte “Definição de configurações do Credential Manager na página 25”.

Registro de um novo aplicativo

O Credential Manager lhe pede para registrar qualquer aplicativo iniciado enquanto você estiver conectado ao Credential Manager. É possível também registrar um aplicativo manualmente.

Utilização do registro automático

1. Abra um aplicativo que exija login.
2. Clique no ícone do programa Credential Manager SSO ou caixa de diálogo de senha no web site.
3. Digite sua senha para o programa ou web site e, em seguida, clique em **OK**. A caixa de diálogo **Credential Manager Single Sign On** (Login único do Credential Manager) é aberta.
4. Clique em **Mais** e selecione a partir das seguintes opções:
   - Não utilizar SSO para esse site ou aplicativo.
   - Solicitar selecionar conta para esse aplicativo.
   - Preencher credenciais, mas não enviar.
   - Usuário autenticado antes de enviar credenciais.
   - Exibir atalho de SSO para esse aplicativo.
5. Clique em **Sim** para completar o registro.

Utilização do registro manual (arrastar e soltar)

1. No HP ProtectTools Security Manager, clique em **Credential Manager** e, em seguida, clique em **Services and Applications** (Serviços e aplicativos) no painel esquerdo.
2. Clique em **Manage Services and Applications** (Gerenciar serviços e aplicativos).

   A caixa de diálogo Credential Manager Single Sign On (Login único do Credential Manager) é exibida.
3. Para modificar ou remover um site da Web ou aplicativo registrado anteriormente, selecione o registro desejado na lista.
4. Siga as instruções na tela.

Gerenciamento de aplicativos e credenciais

Modificação das propriedades do aplicativo

1. No HP ProtectTools Security Manager, clique em **Credential Manager** e, em seguida, clique em **Services and Applications** (Serviços e aplicativos) no painel esquerdo.
2. Clique em **Manage Services and Applications** (Gerenciar serviços e aplicativos).

   A caixa de diálogo Credential Manager Single Sign On (Login único do Credential Manager) é exibida.
3. Clique na entrada do aplicativo que deseja modificar e, em seguida, clique em **Propriedades**.
4. Clique na guia **Geral** para modificar o nome do aplicativo e a descrição. Altere as configurações marcando ou desmarcando as caixas de seleção próximas às configurações apropriadas.
5. Clique na guia **Script** para exibir e editar o script do aplicativo de Single Sign On.
6. Clique em **OK**.

Remoção de um aplicativo do Single Sign On

1. No HP ProtectTools Security Manager, clique em **Credential Manager** e, em seguida, clique em **Services and Applications** (Serviços e aplicativos) no painel esquerdo.
2. Clique em **Manage Services and Applications** (Gerenciar serviços e aplicativos).

   A caixa de diálogo Credential Manager Single Sign On (Login único do Credential Manager) é exibida.
3. Clique no aplicativo que deseja remover e, em seguida, clique em **Remove** (Remover).
4. Clique em **Sim** na caixa de diálogo de confirmação.
5. Clique em **OK**.

Exportação de um aplicativo

É possível exportar aplicativos para criar uma cópia de backup do script de aplicativo do Single Sign On. Este arquivo pode então ser usado para recuperar os dados do Single Sign On. Isso atua como um complemento para o arquivo de backup da identidade, que contém somente as informações de credencial.

Para exportar um aplicativo:

1. No HP ProtectTools Security Manager, clique em **Credential Manager** e, em seguida, clique em **Services and Applications** (Serviços e aplicativos) no painel esquerdo.
2. Clique em **Manage Services and Applications** (Gerenciar serviços e aplicativos).

   A caixa de diálogo Credential Manager Single Sign On (Login único do Credential Manager) é exibida.
3. Clique no aplicativo que deseja exportar e, em seguida, clique em **More** (Mais).
4. Siga as instruções apresentadas na tela para completar a exportação.
5. Clique em **OK**.

Importação de um aplicativo

1. No HP ProtectTools Security Manager, clique em **Credential Manager** e, em seguida, clique em **Services and Applications** (Serviços e aplicativos) no painel esquerdo.
2. Clique em **Manage Services and Applications** (Gerenciar serviços e aplicativos).

   A caixa de diálogo Credential Manager Single Sign On (Login único do Credential Manager) é exibida.
3. Clique no aplicativo que deseja importar e, em seguida, clique em **More** (Mais).
4. Siga as instruções apresentadas na tela para completar a importação.
5. Clique em **OK**.

Modificação de credenciais

1. No HP ProtectTools Security Manager, clique em **Credential Manager** e, em seguida, clique em **Services and Applications** (Serviços e aplicativos).
2. Clique em **Manage Services and Applications** (Gerenciar serviços e aplicativos).

   A caixa de diálogo Credential Manager Single Sign On (Login único do Credential Manager) é exibida.
3. Clique na entrada do aplicativo que deseja modificar e, em seguida, clique em **Mais**.
4. Selecione qualquer uma das seguintes opções:
   - Aplicativos
     - Adicionar novas credenciais
     - Excluir credenciais
     - Propriedades

- Importar Script
- Exportar Script

- Credenciais
  - Criar nova
- Visualizar senha

  NOTA: Você deve autenticar sua identidade antes de visualizar a senha.

5. Siga as instruções na tela.
6. Clique em **OK**.

Utilização de proteção de aplicativos

Este recurso permite que você configure acesso a aplicativos. Você pode restringir o acesso com base no seguinte critério:

- Categoria de usuário
- Tempo de uso
- Inatividade do usuário

Restrição de acesso a um aplicativo

1. No HP ProtectTools Security Manager, clique em **Credential Manager** no painel esquerdo e, em seguida, clique em **Services and Applications** (Serviços e aplicativos).
2. Clique em **Application Protection** (Proteção de aplicativo).
3. Selecione uma categoria de usuário cujo acesso deseja gerenciar.

   NOTA: Se a categoria não é Todos, pode ser necessário selecionar **Substituir configurações padrão** para substituir as configurações para a categoria Todos.

4. Clique em **Add** (Adicionar).

   O Assistente para adicionar programas é exibido.

5. Siga as instruções na tela.

Remoção de proteção de um aplicativo

Para remover restrições de um aplicativo:

1. No HP ProtectTools Security Manager, clique em **Credential Manager** no painel esquerdo.
2. Clique em **Services and Applications** (Serviços e aplicativos).
3. Clique em **Application Protection** (Proteção de aplicativo).
4. Selecione uma categoria de usuário cujo acesso deseja gerenciar.

   NOTA: Se a categoria não é Todos, pode ser necessário clicar em **Substituir configurações padrão** para substituir as configurações para a categoria Todos.

5. Clique na entrada do aplicativo que deseja remover e, em seguida, clique em **Remover**.
6. Clique em **OK**.

Alteração de configurações de restrições para um aplicativo protegido

1. Clique em **Application Protection** (Proteção de aplicativo).
2. Selecione uma categoria de usuário cujo acesso deseja gerenciar.

   NOTA: Se a categoria não é Todos, pode ser necessário clicar em **Substituir configurações padrão** para substituir as configurações para a categoria Todos.

3. Clique no aplicativo que deseja alterar, em seguida clique em **Propriedades**. A caixa de diálogo **Propriedades** desse aplicativo é aberta.
4. Clique na guia **Geral**. Selecione uma destas configurações:
   - Desativada (não pode ser usada)
   - Ativada (pode ser usada sem restrições)
   - Restrito (Uso depende das configurações)
5. Quando selecionar Restrito, as seguintes configurações estão disponíveis:
   a. Se desejar restringir o uso com base no tempo, dia ou data clique na guia **Programar** e configure as definições.
   b. Se desejar restringir o uso com base em inatividade, clique na guia **Avançado** e selecione o período de inatividade.
6. Clique em **OK** para fechar a caixa de diálogo **Properties** (Propriedades) do aplicativo.
7. Clique em **OK**.

Tarefas avançadas (somente administrador)

A página “Autenticação e credenciais” e “Configurações avançadas” do Credential Manager estão disponíveis apenas para estes usuários com direitos de administrador. A partir desta página, você pode desempenhar as seguintes tarefas:

- Especificar como os usuários e administradores efetuam o login
- Configuração de requisitos personalizados de autenticação
- Configuração de propriedades da credencial
- Definição de configurações do Credential Manager

Especificar como os usuários e administradores efetuam o login

Da página “Autenticação e credenciais”, você pode especificar que tipo ou combinação de credenciais é requerida para usuários ou administradores.

Para especificar como os usuários ou administradores efetuam o login:

1. No HP ProtectTools Security Manager, clique em **Credential Manager** no painel esquerdo.
2. Clique em **Multifactor Authentication** (Autenticação de multifatores)
3. No painel direito, clique na guia **Autenticação**.
4. Clique na categoria (**Usuários** ou **Administradores**) na lista de categorias.
5. Clique no tipo ou combinação de métodos de autenticação da lista.
6. Clique em **Aplicar** e, em seguida, clique em **OK**.

Configuração de requisitos personalizados de autenticação

Se a definição da autenticação de credenciais que deseja não está listada na guia Autenticação da página “Autenticação e credenciais”, você pode criar requisitos personalizados.

Para configurar requisitos personalizados:

1. No HP ProtectTools Security Manager, clique em **Credential Manager** no painel esquerdo.
2. Clique em **Multifactor Authentication** (Autenticação de multifatores).
3. No painel direito, clique na guia **Autenticação**.
4. Clique na categoria (**Usuários** ou **Administradores**) na lista de categorias.
5. Clique em **Personalizar** na lista de métodos de autenticação.
6. Clique em **Configurar**.
7. Selecione os métodos de autenticação que deseja utilizar.
8. Selecione a combinação de métodos clicando em uma das seguintes seleções:
   - Usar E para combinar os métodos de autenticação

     (Os usuários terão que autenticar com todos os métodos selecionados sempre que efetuarem o login.)
   - Use OU para requerer um de dois ou mais métodos de autenticação

     (Os usuários poderão escolher qualquer um dos métodos selecionados sempre que efetuarem o login.)
9. Clique em **OK**.
10. Clique em **Aplicar** e, em seguida, clique em **OK**.

Configuração de propriedades da credencial

Da guia Credenciais da página “Autenticação e credenciais”, você pode visualizar a lista de métodos de autenticação disponível e modificar as configurações.

Para configurar as credenciais:

1. No HP ProtectTools Security Manager, clique em **Credential Manager** no painel esquerdo.
2. Clique em **Multifactor Authentication** (Autenticação de multifatores).
3. Clique na guia **Credentials** (Credenciais).

4. Clique no tipo de credencial que deseja modificar. É possível modificar a credencial utilizando uma das seguintes opções:
   - Para registrar a credencial, clique em **Registrar** e siga as instruções apresentadas na tela.
   - Para excluir uma credencial, clique em **Limpar** e, em seguida, clique em **Sim** na caixa de diálogo de confirmação.
   - Para modificar as propriedades da credencial, clique em **Propriedades** e, em seguida, siga as instruções apresentadas na tela.
5. Clique em **Aplicar** e, em seguida, clique em **OK**.

Definição de configurações do Credential Manager

Na página “Advanced Settings” (Configurações Avançadas), é possível acessar e modificar diversas configurações utilizando as seguintes guias:

- Geral—Permite modificar as configurações para configuração básica.
- Single Sign On—Permite modificar as configurações sobre como um Single Sign On funciona para o usuário atual, assim como se gerencia a detecção de telas de login, login automático para diálogos de login registrados e exibição de senha.
- Serviços e aplicativos—Permite a você visualizar os serviços disponíveis e modificar as configurações destes serviços.
- Segurança—Permite a você selecionar o software do leitor de impressão digital e ajustar o nível de segurança do leitor de impressão digital.
- Smart cards e tokens — Permite a você visualizar e modificar as propriedades de todos os Java Cards e tokens disponíveis.

Para modificar as configurações do Credential Manager:

1. No HP ProtectTools Security Manager, clique em **Credential Manager** no painel esquerdo.
2. Clique em **Settings** (Configurações).
3. Clique na guia apropriada para as configurações que deseja modificar:
4. Siga as instruções apresentadas na tela para modificar as configurações.
5. Clique em **Aplicar** e, em seguida, clique em **OK**.

Exemplo 1—Utilizando a página “Configuração avançada” para permitir o login do Windows a partir do Credential Manager

1. No HP ProtectTools Security Manager, clique em **Credential Manager** no painel esquerdo.
2. Clique em **Settings** (Configurações).
3. Clique na guia **General** (Geral).
4. Em **Selecione a maneira na qual os usuários fazem logon no Windows (requer reinicialização)**, marque a caixa de seleção **Use Credential Manager com solicitação de logon clássica**.

5. Clique em **Aplicar** e, em seguida, clique em **OK**.
6. Reinicie o computador.

NOTA: Marcar a caixa de seleção **Use Credential Manager com solicitação de logon clássica** permite que você bloqueie seu computador. Consulte "Bloqueio do computador (estação de trabalho) na página 17".

Exemplo 2—Utilizar a página “Configuração avançada” para exigir verificação do usuário antes do Single Sign On

1. No HP ProtectTools Security Manager, clique em **Credential Manager** e, em seguida, clique em **Settings** (Configurações).
2. Clique na guia **Single Sign On**.
3. Em **Quando a caixa de diálogo de logon registrado ou a página da web é detectada**, marque a caixa de seleção **Autenticar usuário antes de enviar credenciais**.
4. Clique em **Aplicar** e, em seguida, clique em **OK**.
5. Reinicie o computador.

3 Drive Encryption for HP ProtectTools (somente em determinados modelos)

△ **CUIDADO:** Se decidir desinstalar o módulo Drive Encryption, você deve primeiro descriptografar todas as unidades criptografadas. Se isso não for feito, não será possível acessar os dados nas unidades criptografadas a menos que você tenha se registrado no serviço de recuperação do Drive Encryption. A reinstalação do módulo Drive Encryption não permitirá a você acessar as unidades criptografadas.

Procedimentos de configuração

Abertura do Drive Encryption

1. Clique em Iniciar, Todos os Programas e, em seguida, clique em **HP ProtectTools Security Manager**.
2. Clique em **Drive Encryption**.

Tarefas básicas

Ativação do Drive Encryption

Use o assistente de instalação do HP ProtectTools Security Manager para ativar o Drive Encryption.

Desativação do Drive Encryption

Use o assistente de instalação do HP ProtectTools Security Manager para desativar o Drive Encryption.

Login após o Drive Encryption ser ativado

É preciso efetuar login na tela de login do Drive Encryption quando o computador é ligado após o Drive Encryption ter sido ativado e sua conta de usuário ter sido registrada:

NOTA: Se o administrador do Windows houver ativado o recurso Pre-boot Security (segurança pré-início) no HP ProtectTools Security Manager, você fará o login no computador assim que ele for ligado, e não na tela de login do Drive Encryption.

1. Selecione seu nome de usuário e, em seguida, digite sua senha do Windows, informe seu PIN do Java™ Card ou forneça uma impressão digital registrada.
2. Clique em **OK**.

NOTA: Se utilizar uma chave de recuperação para efetuar login na tela de login do Drive Encryption, você será solicitado também a selecionar seu nome de usuário do Windows e digitar sua senha na tela de login do Windows.

Tarefas avançadas

Gerenciamento do Drive Encryption (tarefa do administrador)

A página “Encryption Management” (Gerenciamento de criptografia) permite aos administradores do Windows visualizarem e alterarem o status do Drive Encryption (ativo ou inativo) e visualizarem o status de criptografia de todas as unidades de disco rígido do computador.

Ativação de uma senha protegida por TPM (somente em determinados modelos)

Use a ferramenta Embedded Security no HP ProtectTools para ativar o TPM. Após a ativação, o processo de login na tela de login do Drive Encryption solicitará o nome de usuário e a senha do Windows.

NOTA: Devido à senha ser protegida por um chip de segurança TPM, se a unidade de disco rígido for movida para outro computador, os dados não poderão ser acessados a menos que as configurações do TPM sejam migradas para esse computador.

1. Use a ferramenta Embedded Security no HP ProtectTools para ativar o TPM.
2. Abra o Drive Encryption e clique em **Encryption Management** (Gerenciamento de criptografia).
3. Marque a caixa de seleção **TPM-protected password** (Senha protegida por TPM).

Criptografia ou descriptografia de unidades individuais

1. Abra o Drive Encryption e clique em **Encryption Management** (Gerenciamento de criptografia).
2. Clique em **Change Encryption** (Alterar criptografia).
3. Na caixa de diálogo Change Encryption (Alterar criptografia), marque ou desmarque a caixa de seleção próxima a cada unidade de disco rígido que deseja criptografar ou descriptografar e, em seguida, clique em **OK**.

NOTA: Quando a unidade está sendo criptografada ou descriptografada, a barra de progresso exibe o tempo restante para concluir o processo durante a sessão atual. Se o computador for desligado ou iniciar a suspensão ou a hibernação durante o processo de criptografia e, em seguida, for reiniciado, o campo Tempo restante exibido é reiniciado mas a criptografia é retomada de onde foi interrompida. A exibição do tempo restante e do progresso se alterará mais rapidamente para refletir o progresso anterior.

Backup e recuperação (tarefa do administrador)

A página “Recovery” (Recuperação) permite aos administradores do Windows fazerem o backup e a recuperação de chaves de criptografia.

Criação de chaves de backup

CUIDADO: Certifique-se de guardar o dispositivo de armazenamento com a chave de backup em um local seguro, pois se esquecer a sua senha ou perder seu Java Card, este dispositivo será sua única forma de acesso ao disco rígido.

1. Abra o Drive Encryption e, em seguida, clique em **Recovery** (Recuperação).
2. Clique em **Backup Keys** (Chaves de backup).

3. Na página “Select Backup Disk” (Selecione o disco de backup), clique no nome do dispositivo em que deseja fazer o backup da chave de criptografia, em seguida clique em **Next** (Avançar).

4. Leia as informações na próxima página exibida e, em seguida, clique em **Next** (Avançar).

   A chave de criptografia é salva no dispositivo de armazenamento selecionado.

5. Clique em **OK** quando a caixa de diálogo de confirmação for exibida.

Registro para recuperação on-line

O Serviço de recuperação on-line de chave do Drive Encryption armazena uma cópia backup de sua chave de criptografia, que permitirá a você acessar o computador caso esqueça sua senha e não tenha acesso a seu backup local.

NOTA: Você deve estar conectado à Internet e ter um endereço de e-mail válido para registrar e recuperar sua senha através desse serviço.

1. Abra o Drive Encryption e, em seguida, clique em **Recovery** (Recuperação).

2. Clique em **Register** (Registrar).

3. Clique em uma das seguintes opções:

   - I want to create a new recovery account for this PC (Eu desejo criar uma nova conta de recuperação para este PC). Se escolher essa opção, digite seu endereço de e-mail e outras informações, e em seguida clique em **Next** (Avançar).

   - I want to add this PC to my existing web recovery account (Eu quero adicionar este PC a uma conta existente de recuperação na Web).

4. Crie e confirme uma senha, selecione as perguntas de segurança e digite as respostas, em seguida, clique em **Next** (Avançar).

   NOTA: Um código de ativação de conta será enviado para o endereço de e-mail fornecido.

5. Insira o código de ativação e clique em **Next** (Avançar).

6. Insira o número de série do computador e clique em **Next** (Avançar).

   NOTA: Para localizar o número de série do computador, clique em **Iniciar** e, em seguida, clique em **Ajuda e Suporte**.

7. Se você não possui um cupom de assinatura, clique no link **Click here to purchase coupons** (Clique aqui para adquirir cupons).

   Ao clicar no link você será direcionado ao site da Web do serviço de recuperação SafeBoot. Não saia do assistente.

8. Clique em **Comprar Cupons**.

9. Selecione seu país, o tipo de computador e, em seguida, clique em **Iniciar**.

10. Clique em **Comprar** ao lado das opções de assinatura de 1 ou 3 anos.

11. Clique em **Fechamento**.

12. Leia os termos e condições e, em seguida, clique em **Aceito**.

13. Insira suas informações de cobrança e, em seguida, clique em **Continuar**.

14. Insira informações sobre o seu cartão de crédito e, em seguida, clique em **Make Payment** (Efetuar pagamento).
15. Anote seu código de cupom e retorne à página “Account Activation” (Ativação de conta) do assistente.
16. Insira o código de ativação de conta e clique em **Next** (Avançar).
17. Quando a caixa de diálogo de confirmação for exibida, clique em **OK**.

Gerenciamento de uma conta de recuperação on-line existente

Depois de criar uma conta de recuperação on-line, você poderá acessar o site da Web do serviço de recuperação do SafeBoot para recuperar o acesso ao seu computador, caso tenha perdido sua senha, modificar suas configurações pessoais, redefinir a senha usada para a conta de recuperação on-line e visualizar ou renovar sua conta.

1. Abra o Drive Encryption e, em seguida, clique em **Recovery** (Recuperação).
2. Clique em **Manage** (Gerenciar).
3. Quando a página da Web "Serviço de Recuperação do SafeBoot" for exibida, clique em **Administrar conta** ou **Processo de Recuperação**.
4. Na página de login do serviço de recuperação, insira seu endereço de e-mail, senha e os números e letras que aparecem na caixa.
5. Clique em **Login**.
6. Clique em **Profile** (Perfil) para atualizar suas informações pessoais, como telefone ou endereço de cobrança.

   – ou –

   Clique em **Reset Password** (Redefinir senha) para redefinir ou alterar sua senha.

   – ou –

   Clique em **My Subscriptions** (Minhas assinaturas) para exibir suas informações de assinatura atuais.

NOTA: A página “My Subscriptions” (Minhas assinaturas) lhe permite também renovar sua assinatura. Clique em **Renew Subscription** (Renovar assinatura) para executar essa ação.

Execução de uma recuperação

Execução de uma recuperação local

1. Ligue o computador.
2. Insira o dispositivo de armazenamento removível para armazenar sua chave de backup.
3. Quando a caixa de diálogo de login do Drive Encryption for HP ProtectTools for exibida, clique em **Cancel** (Cancelar).
4. Clique em **Options** (Opções) no canto inferior esquerdo da tela e, em seguida, clique em **Recovery** (Recuperação).
5. Clique em **Local recovery** (Recuperação local) e, em seguida, clique em **Next** (Avançar).

6. Selecione o arquivo que contém sua chave de backup ou clique em **Browse** (Procurar) para procurá-lo e, em seguida, clique em **Next** (Avançar).
7. Quando a caixa de diálogo de confirmação for exibida, clique em **OK**.

   O processo de recuperação é concluído e o computador é iniciado.

NOTA: É altamente recomendável redefinir sua senha após executar uma recuperação.

Execução de uma recuperação on-line

NOTA: Esta seção descreve como executar uma recuperação on-line quando você tem acesso a um outro computador com conexão com a Internet. Se você não tiver acesso a um computador assim, entre em contato com o suporte técnico da HP.

1. Ligue o computador.
2. Quando a caixa de diálogo de login do Drive Encryption for HP ProtectTools for exibida, clique em **Cancel** (Cancelar).
3. Clique em **Options** (Opções) no canto inferior esquerdo da tela e, em seguida, clique em **Recovery** (Recuperação).
4. Clique em **Web recovery** (Recuperação pela Web) e, em seguida, clique em **Next** (Avançar).
5. Grave o código de cliente e clique em **Next** (Avançar).
6. Em um computador diferente com uma conexão com a Internet, acesse o site da Web do Serviço de Recuperação do SafeBoot em http://www.safeboot-hp.com.
7. Clique em **Processo de Recuperação**.
8. Na página de login do serviço de recuperação, insira seu endereço de e-mail, senha e os números e letras que aparecem na caixa.
9. Clique em **Login**.
10. Clique em **Processo de Recuperação**.
11. Insira o código de cliente que você anotou, obtido no computador que está tentando recuperar, e insira os números e letras exibidos na caixa.
12. Clique em **Submit** (Enviar).
13. Grave cada linha da chave de resposta.
14. No computador que você está tentando recuperar, insira a linha 1 da chave de resposta que você gravou do site da Web do serviço de recuperação SafeBoot e clique em **Enter**.
15. Insira a linha 2 da chave de resposta e, em seguida, clique em **Enter**.
16. Insira a linha 3 da chave de resposta e, em seguida, clique em **Enter**.
17. Insira a linha 4 da chave de resposta e, em seguida, clique em **Enter**.

    NOTA: A linha 4 da chave de resposta é mais curta que as 3 primeiras linhas.
18. Clique em **Finish** (Concluir).

NOTA: É altamente recomendável redefinir sua senha após executar uma recuperação.

4 Privacy Manager for HP ProtectTools (somente em determinados modelos)

O Privacy Manager for HP ProtectTools permite usar métodos avançados de login de segurança (autenticação) para verificar a origem, integridade e segurança da comunicação ao utilizar e-mail, documentos do Microsoft® Office ou troca de mensagens instantâneas.

O Privacy Manager alavanca a infra-estrutura de segurança fornecida pelo HP ProtectTools Security Manager, que inclui os seguintes métodos de login:

- Autenticação por impressão digital
- Senha do Windows®
- HP ProtectTools Java™ Card

É possível usar qualquer um dos métodos de login de segurança acima no Privacy Manager.

Abertura do Privacy Manager

Para abrir o Privacy Manager:

1. Clique em **Iniciar**, **Todos os Programas** e **HP ProtectTools Security Manager**.
2. Clique em **Privacy Manager: Sign and Chat**.

– ou –

Clique com o botão direito no ícone **HP ProtectTools** na área de notificação, à direita da barra de tarefas, clique em **Privacy Manager: Sign and Chat** e, em seguida, clique em **Configuration** (Configuração).

– ou –

Na barra de ferramentas de uma mensagem de e-mail do Microsoft Outlook, clique na seta para baixo perto de **Send Securely** (Enviar em Segurança) e depois clique em **Certificate Manager** (Gerenciador de Certificados) ou **Trusted Contact Manager** (Gerenciador de Contatos Confiáveis).

– ou –

Na barra de ferramentas de um documento do Microsoft Office, clique na seta para baixo perto de **Sign and Encrypt** (Assinar e Criptografar) e depois clique em **Certificate Manager** (Gerenciador de Certificados) ou **Trusted Contact Manager**.

Procedimentos de configuração

Gerenciamento de certificados do Privacy Manager

Os certificados do Privacy Manager protegem dados e mensagens usando uma tecnologia de criptografia conhecida como PKI (Public Key Infrastructure - Infra-estrutura de chave pública). PKI exige que os usuários obtenham chaves de criptografia e um Certificado do Privacy Manager emitido por uma autoridade certificadora (certificate authority - CA). Diferente da maioria dos softwares de criptografia e autenticação de dados que requer somente autenticação periódica, o Privacy Manager requer autenticação toda vez que você assina uma mensagem de e-mail ou um documento do Microsoft Office com uma chave criptografada. O Privacy Manager torna seguro o processo de salvar e enviar suas informações importantes.

Solicitação e instalação de um Certificado do Privacy Manager

Antes que você possa utilizar os recursos do Privacy Manager, precisa solicitar e instalar um Certificado do Privacy Manager (a partir do Privacy Manager) utilizando um endereço de e-mail válido. O endereço de e-mail precisa ser ajustado como uma conta dentro do Microsoft Outlook no mesmo computador a partir do qual você está solicitando um Certificado do Privacy Manager.

Solicitação de um Certificado do Privacy Manager

1. Abra o Privacy Manager e clique em **Certificate Manager** (Gerenciador de Certificados).
2. Clique em **Request a Privacy Manager Certificate** (Solicitar um Certificado do Privacy Manager).
3. Na página “Welcome” (Bem-vindo), leia o texto e, em seguida, clique em **Next** (Avançar).
4. Na página “License Agreement” (Contrato de licença), leia o contrato de licença.
5. Certifique-se de que a caixa de seleção perto de **Check here to accept the terms of this license agreement** (Marque aqui para aceitar os termos deste contrato de licença) esteja selecionada e depois clique em **Next** (Avançar).
6. Na página “Your Certificate Details” (Detalhes do seu certificado), digite as informações necessárias e depois clique em **Next** (Avançar).
7. Na página “Certificate Request Accepted” (Solicitação de certificado aceita), clique em **Finish** (Concluir).

   Você vai receber um e-mail no Microsoft Outlook com seu Certificado do Privacy Manager anexado.

Instalação de um Certificado do Privacy Manager

1. Quando você receber o e-mail com seu Certificado do Privacy Manager anexado, abra o e-mail e clique no botão **Setup** (Configurar), no canto inferior direito da mensagem.
2. Faça a autenticação utilizando o método de login de segurança de sua escolha.
3. Clique em **Next** (Avançar) na página “Certificate Installed” (Certificado instalado).
4. Na página “Certificate Backup” (Backup de certificado), digite uma localização e um nome para o arquivo de backup, ou clique em **Browse** (Procurar) para procurar uma localização.

CUIDADO: Verifique se salvou o arquivo em um outro local além da sua unidade de disco rígido e guarde-o em um local seguro. Este arquivo deve ser apenas para o seu uso, e será necessário caso precise restaurar seu Certificado do Privacy Manager e as chaves associadas.

5. Insira e confirme uma senha e, em seguida, clique em **Next** (Avançar).
6. Faça a autenticação utilizando o método de login de segurança de sua escolha.
7. Se você deseja iniciar o processo de convite de um contato confiável, siga as instruções apresentadas na tela.

   – ou –

   Se você clicar em Cancel (Cancelar), consulte Gerenciamento de contatos confiáveis para obter informações sobre como acrescentar um contato confiável posteriormente.

Exibição de detalhes do Certificado do Privacy Manager

1. Abra o Privacy Manager e clique em **Certificate Manager** (Gerenciador de Certificados).
2. Clique em um Certificado do Privacy Manager.
3. Clique em **Certificate details** (Detalhes do certificado).
4. Quando você houver terminado de ver os detalhes, clique em **OK**.

Renovação de um Certificado do Privacy Manager

Quando seu Certificado do Privacy Manager estiver para expirar, você será notificado de que precisa renová-lo:

1. Abra o Privacy Manager e clique em **Certificate Manager** (Gerenciador de Certificados).
2. Clique em um Certificado do Privacy Manager.
3. Clique em **Renew certificate** (Renovar certificado).
4. Siga as instruções apresentadas na tela para comprar um novo Certificado do Privacy Manager.

NOTA: O processo de renovação do Certificado do Privacy Manager não substitui o seu Certificado do Privacy Manager antigo. Você vai precisar comprar um novo Certificado do Privacy Manager e instalá-lo utilizando os mesmos procedimentos descritos em Solicitação e instalação de um Certificado do Privacy Manager.

Configuração de um Certificado do Privacy Manager padrão

Apenas Certificados do Privacy Manager são visíveis de dentro do Privacy Manager, mesmo se certificados adicionais de outras autoridades certificadoras estiverem instalados no seu computador.

Caso você tenha mais de um Certificado do Privacy Manager no seu computador que foram instalados a partir do Privacy Manager, você pode especificar um deles como o certificado padrão:

1. Abra o Privacy Manager e clique em **Certificate Manager** (Gerenciador de Certificados).
2. Clique no Certificado do Privacy Manager que deseja utilizar como padrão e em seguida clique em **Set default** (Definir Padrão).
3. Clique em **OK**.

NOTA: Você não precisa usar o seu Certificado do Privacy Manager padrão. A partir das várias funções do Privacy Manager, você pode selecionar qualquer um dos seus Certificados do Privacy Manager para uso.

Exclusão de um Certificado do Privacy Manager

Se você excluir um Certificado do Privacy Manager, não vai poder abrir quaisquer arquivos ou ver quaisquer dados que tenha criptografado com aquele certificado. Se você excluiu acidentalmente um Certificado do Privacy Manager, pode restaurá-lo utilizando o arquivo de backup que criou quando instalou o certificado.

Para excluir um Certificado do Privacy Manager:

1. Abra o Privacy Manager e clique em **Certificate Manager** (Gerenciador de Certificados).
2. Clique no Certificado do Privacy Manager que deseja excluir e em seguida clique em **Advanced** (Avançado).
3. Clique em **Delete** (Excluir).
4. Quando a caixa de diálogo de confirmação for exibida, clique em **Yes** (Sim).
5. Clique em **Close** (Fechar) e em **Apply** (Aplicar).

Restauração de um Certificado do Privacy Manager

Se você excluiu acidentalmente um Certificado do Privacy Manager, pode restaurá-lo utilizando o arquivo de backup que criou quando instalou ou exportou o certificado:

1. Abra o Privacy Manager e clique em **Migration** (Migração).
2. Clique em **Import migration file** (Importar arquivo de migração).
3. Na página “Migration File” (“Arquivo de Migração”), clique em **Browse** (Procurar) para buscar o arquivo .dppsm que você criou quando instalou ou exportou o Certificado do Privacy Manager e depois clique em **Next** (Avançar).
4. Na página “Migration File Import” (Importar Arquivo de Migração), clique em **Finish** (Concluir).
5. Clique em **Close** (Fechar) e em **Apply** (Aplicar).

NOTA: Para obter mais informações, consulte Instalação de um Certificado do Privacy Manager ou Exportação de Certificados do Privacy Manager e de Contatos Confiáveis.

Revogação do seu Certificado do Privacy Manager

Se você acha que a segurança do seu Certificado do Privacy Manager foi ameaçada, você pode revogar seu próprio certificado:

NOTA: Um Certificado do Privacy Manager revogado não é excluído. O certificado ainda pode ser utilizado para ver arquivos que estão criptografados.

1. Abra o Privacy Manager e clique em **Certificate Manager** (Gerenciador de Certificados).
2. Clique em **Advanced** (Avançado).
3. Clique no Certificado do Privacy Manager que deseja revogar e em seguida clique em **Revoke** (Revogar).

4. Quando a caixa de diálogo de confirmação for exibida, clique em **Yes** (Sim).
5. Faça a autenticação utilizando o método de login de segurança de sua escolha.
6. Siga as instruções na tela.

Gerenciamento de contatos confiáveis

Contatos confiáveis são usuários com quem você trocou Certificados do Privacy Manager, permitindo que vocês se comuniquem em segurança.

Adição de contatos confiáveis

1. Você envia um convite por e-mail para um destinatário do tipo Trusted Contact (Contato Confiável).
2. O destinatário Trusted Contact (Contato Confiável) responde ao e-mail.
3. Você recebe o e-mail de resposta do destinatário Trusted Contact (Contato Confiável) e clica em Accept (Aceitar).

Você pode enviar e-mails de convite de Trusted Contact (Contato Confiável) para destinatários individuais ou pode enviar o convite a todos os contatos na sua lista de endereços do Microsoft Outlook.

NOTA: Para responder ao seu convite e tornar-se um Trusted Contact (Contato Confiável), os destinatários Trusted Contact (Contato Confiável) precisam ter o Privacy Manager instalado nos seus computadores ou ter um cliente alternativo instalado. Para obter informações sobre como instalar o cliente alternativo, acesse o site da Web do DigitalPersona em http://DigitalPersona.com/PrivacyManager.

Adição de um contato confiável

1. Abra o Privacy Manager, clique em **Trusted Contacts Manager** (Gerenciador de Contatos Confiáveis) e depois clique em **Invite Contacts** (Convidar Contatos).

   – ou –

   No Microsoft Outlook, clique na seta para baixo perto de **Send Securely** (enviar em Segurança) e depois clique em **Invite Contacts** (Convidar Contatos).
2. Se a caixa de diálogo Select Certificate (Selecionar Certificado) abrir, clique no Certificado do Privacy Manager que deseja utilizar e em seguida clique em **OK**.
3. Quando a caixa de diálogo Trusted Contact Invitation (Convite de Contato Confiável) for exibida, leia o texto e clique em **OK**.

   Um e-mail será gerado automaticamente.
4. Digite um ou mais endereços de e-mail dos recipientes que deseja acrescentar como Trusted Contacts (Contatos Confiáveis).
5. Edite o texto e assine o seu nome (opcional).
6. Clique em **Send** (Enviar).

   NOTA: Caso não tenha obtido um certificado do Privacy Manager, uma mensagem informa você de que deve ter um certificado do Privacy Manager para que possa enviar uma solicitação de Trusted Contact (Contato Confiável). Clique em OK para iniciar o Certificate Request Wizard (Assistente de Solicitação de Certificado).

7. Faça a autenticação utilizando o método de login de segurança de sua escolha.
8. Quando receber um e-mail de resposta de um destinatário aceitando o convite para tornar-se um Trusted Contact (Contato Confiável), clique em Accept (Aceitar) no canto inferior direito do e-mail.

   Será exibida uma caixa de diálogo, confirmando que o destinatário foi acrescentado com sucesso à sua lista de Trusted Contacts (Contatos Confiáveis).
9. Clique em **OK**.

Adição de contatos confiáveis usando sua lista de endereços do Microsoft Outlook

1. Abra o Privacy Manager, clique em **Trusted Contacts Manager** (Gerenciador de Contatos Confiáveis) e depois clique em **Invite Contacts** (Convidar Contatos).

   – ou –

   No Microsoft Outlook, clique na seta para baixo perto de **Send Securely** (Enviar em Segurança) e depois clique em **Invite All My Outlook Contacts** (Convidar Todos os Meus Contatos do Outlook).
2. Quando a página “Trusted Contact Invitation” (Convite de Contato Confiável) abrir, selecione os endereços de e-mail dos destinatários que deseja acrescentar como Trusted Contacts (Contatos Confiáveis) e depois selecione **Next** (Avançar).
3. Quando a página “Sending Invitation” (Enviar Convite) for exibida, clique em **Finish** (Concluir).

   Um e-mail listando os endereços de e-mail selecionados do Microsoft Outlook será gerado automaticamente.
4. Edite o texto e assine o seu nome (opcional).
5. Clique em **Send** (Enviar).

   NOTA: Caso não tenha obtido um certificado do Privacy Manager, uma mensagem informa você de que deve ter um certificado do Privacy Manager para que possa enviar uma solicitação de Trusted Contact (Contato Confiável). Clique em **OK** para iniciar o Certificate Request Wizard (Assistente de Solicitação de Certificado).
6. Faça a autenticação utilizando o método de login de segurança de sua escolha.

   NOTA: Quando o e-mail é recebido pelo destinatário de Trusted Contact (Contato Confiável), o destinatário precisa abrir o e-mail e clicar em Accept (Aceitar) no canto inferior esquerdo do e-mail e depois clicar em OK quando a caixa de diálogo de confirmação abrir.
7. Quando receber um e-mail de resposta de um destinatário aceitando o convite para tornar-se um Trusted Contact (Contato Confiável), clique em Accept (Aceitar) no canto inferior direito do e-mail.

   Será exibida uma caixa de diálogo, confirmando que o destinatário foi acrescentado com sucesso à sua lista de Trusted Contacts (Contatos Confiáveis).
8. Clique em **OK**.

Visualização de detalhes de contatos confiáveis

1. Abra o Privacy Manager e clique em **Trusted Contacts Manager** (Gerenciador de Contatos Confiáveis).
2. Clique em um Trusted Contact (Contato Confiável).

3. Clique em **Contact details** (Detalhes de Contato).
4. Quando você houver terminado de ver os detalhes, clique em **OK**.

Exclusão de um contato confiável

1. Abra o Privacy Manager e clique em **Trusted Contacts Manager** (Gerenciador de Contatos Confiáveis).
2. Clique no Trusted Contact (Contato Confiável) que deseja excluir.
3. Clique em **Delete contact** (Excluir Contato).
4. Quando a caixa de diálogo de confirmação for exibida, clique em **Yes** (Sim).

Verificação do status de revogação de um contato confiável

1. Abra o Privacy Manager e clique em **Trusted Contacts Manager** (Gerenciador de Contatos Confiáveis).
2. Clique em um Trusted Contact (Contato Confiável).
3. Clique no botão **Advanced** (Avançado).

   A caixa de diálogo Advanced Trusted Contact Management (Gerenciamento Avançado de Contatos Confiáveis) é exibida.
4. Clique em **Check Revocation** (Verificar Revogação).
5. Clique em **Close** (Fechar).

Tarefas básicas

Utilização do Privacy Manager no Microsoft Office

Depois de instalar o seu Certificado do Privacy Manager, um botão Sign and Encrypt (Assinar e Criptografar) é exibido no lado direito da barra de ferramentas de todos os documentos do Microsoft Word, Microsoft Excel e Microsoft PowerPoint.

Configuração do Privacy Manager em um documento do Microsoft Office

1. Abra o Privacy Manager, clique em **Settings** (Configurações) e depois clique na guia **Documents** (Documentos).

   – ou –

   Na barra de ferramentas de uma mensagem de um documento do Microsoft Office, clique na seta para baixo perto de **Sign and Encrypt** (Assinar e Criptografar) e depois clique em **Settings** (Configurações).

2. Selecione as ações que deseja configurar, em seguida clique em **OK**.

Assinatura de um documento do Microsoft Office

1. No Microsoft Word, Microsoft Excel ou Microsoft PowerPoint, crie e salve um documento.
2. Clique na seta para baixo próxima a **Sign and Encrypt** (Assinar e Criptografar) e em seguida clique em **Sign Document** (Assinar Documento).
3. Faça a autenticação utilizando o método de login de segurança de sua escolha.
4. Quando a caixa de diálogo de confirmação for exibida, leia o texto e clique em **OK**.

Se depois você decidir editar o documento, siga estas etapas:

1. Clique no botão **Office** no canto superior esquerdo da tela.
2. Clique em **Prepare** (Preparar) e depois clique em **Mark as Final** (Marcar como Final).
3. Quando a caixa de diálogo de confirmação for exibida, clique em **Yes** (Sim) para continuar trabalhando.
4. Quando completar sua edição, assine novamente o documento.

Adição de uma linha de assinatura ao assinar um documento do Microsoft Word ou Microsoft Excel

O Privacy Manager permite acrescentar uma linha de assinatura quando você assina um documento do Microsoft Word ou Microsoft Excel:

1. Crie e salve um documento no Microsoft Word ou Microsoft Excel.
2. Clique no menu **Home** (Inicial).
3. Clique na seta para baixo próxima a **Sign and Encrypt** (Assinar e Criptografar) e em seguida clique em **Add Signature Line Before Signing** (Acrescentar Linha de Assinatura Antes de Assinar).

NOTA: Uma marca de seleção é exibida junto a Add Signature Line Before Signing (Acrescentar Linha de Assinatura Antes de Assinar) quando esta opção é selecionada. Esta opção vem ativada como padrão.

4. Clique na seta para baixo próxima a **Sign and Encrypt** (Assinar e Criptografar) e em seguida clique em **Sign Document** (Assinar Documento).

5. Faça a autenticação utilizando o método de login de segurança de sua escolha.

Adição de assinantes sugeridos a um documento do Microsoft Word ou Microsoft Excel

Você pode acrescentar mais de uma linha de assinatura ao seu documento indicando assinantes sugeridos. Um assinante sugerido é um usuário designado pelo proprietário de um documento do Microsoft Word ou do Microsoft Excel para acrescentar uma linha de assinatura ao documento. Os assinantes sugeridos podem ser você ou qualquer outra pessoa que você queira que assine seu documento. Por exemplo, se você preparou um documento que precisa ser assinado por todos os membros do seu departamento, pode incluir linhas de assinatura para esses usuários na parte inferior da página final do documento, com instruções para assiná-lo em uma data específica.

Para acrescentar um assinante sugerido a um documento do Microsoft Word ou Microsoft Excel:

1. Crie e salve um documento no Microsoft Word ou Microsoft Excel.

2. Clique no menu **Insert** (Inserir).

3. No grupo **Text** (Texto) na barra de ferramentas, clique na seta para baixo perto de **Signature Line** (Linha de Assinatura) e depois clique em **Privacy Manager Signature Provider** (Provedor de Assinatura do Privacy Manager).

   A caixa de diálogo Signature (Assinatura) é exibida.

4. Na caixa sob **Suggested signer** (Assinante Sugerido), insira o nome do assinante sugerido.

5. Na caixa sob **Instructions to the signer** (Instruções para o assinante), insira uma mensagem para este assinante sugerido.

NOTA: Esta mensagem vai aparecer no lugar de um título e será excluída ou substituída pelo título do usuário quando o documento for assinado.

6. Selecione a caixa de seleção **Show sign date in signature line** (Exibir data de assinatura na linha de assinatura) para mostrar a data.

7. Selecione a caixa de seleção **Show signer's title in signature line** (Exibir título do assinante na linha de assinatura) para mostrar o título.

NOTA: Como o proprietário do documento designa assinantes sugeridos para seu documento, se as caixas de seleção **Show sign date in signature line** (Exibir data de assinatura na linha de assinatura) e/ou **Show signer's title in signature line** (Exibir título do assinante na linha de assinatura) não forem selecionadas, o assinante sugerido não será capaz de exibir a data e/ou título na linha de assinatura, mesmo que as configurações do documento do assinante sugerido estejam configuradas para fazê-lo.

8. Clique em **OK**.

Adição de um assinante sugerido à linha de assinatura

Quando assinantes sugeridos abrirem o documento, verão seu nome entre parênteses, indicando que a sua assinatura é necessária.

Para assinar o documento:

1. Clique duas vezes na linha de assinatura apropriada.
2. Faça a autenticação utilizando o método de login de segurança de sua escolha.

   A linha de assinatura será exibida de acordo com as configurações especificadas pelo proprietário do documento.

Criptografia de um documento do Microsoft Office

Você pode criptografar um documento do Microsoft Office para você e para os seus Trusted Contacts (Contatos Confiáveis). Quando você criptografa um documento e o fecha, você e o(s) contato(s) confiável(eis) que selecionou da lista precisam autenticá-lo antes de abri-lo.

Para criptografar um documento do Microsoft Office:

1. No Microsoft Word, Microsoft Excel ou Microsoft PowerPoint, crie e salve um documento.
2. Clique no menu **Home** (Inicial).
3. Clique na seta para baixo próxima a **Sign and Encrypt** (Assinar e Criptografar) e em seguida clique em **Encrypt Document** (Criptografar Documento).

   A caixa de diálogo Trusted Contacts (Contatos Confiáveis) é aberta.

4. Clique no nome de um Trusted Contact (Contato Confiável) que será capaz de abrir o documento e exibir o seu conteúdo.

   NOTA: Para selecionar vários nomes de Trusted Contacts (Contatos Confiáveis), pressione e segure a tecla ctrl e clique em cada nome.

5. Clique em **OK**.
6. Faça a autenticação utilizando o método de login de segurança de sua escolha.

Se depois você decidir editar o documento, siga as etapas em **Assinatura de um documento do Microsoft Office** . Quando a criptografia for removida, você poderá editar o documento. Siga as etapas nesta seção para criptografar o documento novamente.

Remoção da criptografia de um documento do Microsoft Office

Quando remove a criptografia de um documento do Microsoft Office, você e seus Trusted Contacts (Contatos Confiáveis) não precisam mais fazer autenticação para abrir e ver os conteúdos do documento.

Para remover a criptografia de um documento do Microsoft Office:

1. Abra um documento criptografado do Microsoft Word, Microsoft Excel ou Microsoft PowerPoint.
2. Faça a autenticação utilizando o método de login de segurança de sua escolha.
3. Clique no menu **Home** (Inicial).
4. Clique na seta para baixo próxima a **Sign and Encrypt** (Assinar e Criptografar) e em seguida clique em **Remove Encryption** (Remover Criptografia).

Envio de um documento do Microsoft Office criptografado

Você pode conectar um documento criptografado do Microsoft Office a uma mensagem de e-mail sem assinar ou criptografar o próprio e-mail. Para fazer isso, crie e envie um e-mail com um documento criptografado como faria normalmente com um e-mail comum com um arquivo anexado.

Contudo, para o máximo de segurança, é recomendado que você criptografe o e-mail quando anexar um documento criptografado ou assinado do Microsoft Office.

Para enviar um e-mail selado com um documento anexado do Microsoft Office assinado e/ou criptografado, siga estas etapas:

1. No Microsoft Outlook, clique em **New** (Novo) ou **Reply** (Responder).
2. Digite sua mensagem de e-mail.
3. Anexe o documento do Microsoft Office.
4. Consulte Selagem e envio de uma mensagem de e-mail para obter mais instruções.

Visualização de um documento assinado do Microsoft Office

NOTA: Você não precisa ter um Certificado do Privacy Manager para visualizar um documento assinado do Microsoft Office.

Quando um documento assinado do Microsoft Office é aberto, uma caixa de diálogo Signatures (Assinaturas) abre perto do documento, exibindo o nome do usuário que assinou o documento e a data em que foi assinado. Você pode clicar com o botão direito o nome para ver detalhes adicionais.

Visualização de um documento do Microsoft Office criptografado

Para ver um documento criptografado do Microsoft Office em outro computador, o Privacy Manager precisa ser instalado naquele computador. Além disso, você precisa importar o Certificado do Privacy Manager que foi usado para criptografar o arquivo.

Um Trusted Contact (Contato Confiável) que deseje visualizar um documento criptografado do Microsoft Office precisa ter um Privacy Manager Certificate (Certificado do Privacy Manager), e o Privacy Manager precisa ser instalado no seu computador. Além disso, o Trusted Contact (Contato Confiável) precisa ser selecionado pelo proprietário do documento criptografado do Microsoft Office.

Utilização do Privacy Manager no Microsoft Outlook

Quando o Privacy Manager é instalado, um botão Privacy (Privacidade) é exibido na barra de ferramentas do Microsoft Outlook, e um botão Send Securely (Enviar em Segurança) é exibido na barra de ferramentas de cada mensagem de e-mail do Microsoft Outlook.

Configuração do Privacy Manager para Microsoft Outlook

1. Abra o **Privacy Manager**, clique em **Settings** (Configurações) e depois clique na guia **E-mail**.

   – ou –

   Na barra de ferramentas principal do Microsoft Outlook, clique na seta para baixo perto de **Privacy** (Privacidade) e depois clique em **Settings** (Configurações).

   – ou –

   Na barra de ferramentas de uma mensagem de e-mail da Microsoft, clique na seta para baixo perto de **Send Securely** (Enviar em Segurança) e depois clique em **Settings** (Configurações).

2. Selecione as ações que deseja executar quando um e-mail seguro é enviado e em seguida clique em **OK**.

Assinatura e envio de uma mensagem de e-mail

▲ No Microsoft Outlook, clique em **New** (Novo) ou **Reply** (Responder).

▲ Digite sua mensagem de e-mail.

▲ Clique na seta para baixo próxima a **Send Securely** (Enviar em Segurança) e em seguida clique em **Sign and Send** (Assinar e Enviar).

▲ Faça a autenticação utilizando o método de login de segurança de sua escolha.

Selagem e envio de uma mensagem de e-mail

Mensagens de e-mail seladas que são digitalmente assinadas e seladas (criptografadas) só podem ser visualizadas pelas pessoas escolhidas por você na sua lista de Trusted Contacts (Contatos Confiáveis).

Para selar e enviar uma mensagem de e-mail para um Trusted Contact (Contato Confiável):

1. No Microsoft Outlook, clique em **New** (Novo) ou **Reply** (Responder).
2. Digite sua mensagem de e-mail.
3. Clique na seta para baixo perto de **Send Securely** (Enviar em Segurança) e depois clique em **Seal for Trusted Contacts and Send** (Selar para Contatos Confiáveis e Enviar).
4. Faça a autenticação utilizando o método de login de segurança de sua escolha.

Visualização de uma mensagem de e-mail selada

Quando uma mensagem de e-mail selada é aberta, a etiqueta de segurança é exibida no cabeçalho do e-mail. Esta etiqueta de segurança fornece as seguintes informações:

- Quais credenciais foram utilizadas para verificar a identidade da pessoa que assinou o e-mail
- O produto que foi utilizado para verificar as credenciais da pessoa que assinou o e-mail

Utilização do Privacy Manager no Windows Live Messenger

Adição de uma atividade do Privacy Manager Chat

Para acrescentar o recurso Privacy Manager Chat ao Windows Live Messenger, siga estas etapas:

1. Efetue o login no Windows Live Home.
2. Clique no ícone **Windows Live** e depois clique em **Windows Live Services**.
3. Clique em **Gallery** (Galeria) e, em seguida, clique em **Messenger**.
4. Clique em **Activities** (Atividades) e, em seguida, clique em **Safety and Security** (Segurança).
5. Clique em **Privacy Manager Chat** e depois siga as instruções na tela.

Inicialização do Privacy Manager Chat

NOTA: Para que possam utilizar os recursos do Privacy Manager Chat, as duas partes precisam ter o Privacy Manager e um Privacy Manager Certificate (Certificado do Privacy Manager) instalados. Para obter detalhes sobre como instalar um Certificado do Privacy Manager, consulte Solicitação e instalação de um Certificado do Privacy Manager na página 5.

1. Para iniciar o Privacy Manager Chat no Windows Live Messenger, execute um dos seguintes procedimentos:

   a. Clique com o botão direito em um contato on-line no Live Messenger e depois selecione **Start an Activity** (Iniciar uma Atividade).

   b. Clique em **Start Privacy Manager Chat** (Iniciar Privacy Manager Chat).

   – ou –

   a. Clique duas vezes em um contato on-line no Live Messenger e depois clique no menu **Conversation** (Conversa).

   b. Clique em **Action** (Ação) e depois clique em **Start Privacy Manager Chat** (Iniciar Privacy Manager Chat).

   O Privacy Manager envia um convite ao contato para iniciar o Privacy Manager Chat. Quando o contato aceita o convite, a janela do Privacy Manager Chat é aberta. Caso o contato convidado não tenha o Privacy Manager, ele será solicitado a baixá-lo.

2. Clique em **Start** (Iniciar) para iniciar uma sessão de bate-papo segura.

Configuração do Privacy Manager Chat para o Windows Live Messenger

1. No Privacy Manager Chat, clique no botão **Settings** (Configurações).

   – ou –

   No Privacy Manager, clique em **Settings** (Configurações) e depois clique na guia **Chat** (Bate-papo).

   – ou –

   No Privacy Manager History Viewer, clique no botão **Settings** (Configurações).

2. Para especificar a quantidade de tempo que o Privacy Manager Chat espera antes de bloquear a sua sessão, selecione um número na caixa **Lock session after _ minutes of inactivity** (Bloquear sessão depois de _ minutos de inatividade).

3. Para especificar uma pasta de histórico para suas sessões de bate-papo, clique em **Browse** (Procurar) para procurar uma pasta e em seguida clique em **OK**.

4. Para automaticamente criptografar e salvar suas sessões quando elas são fechadas, selecione a caixa de seleção **Automatically save secure chat history** (Salvar automaticamente o histórico do bate-papo seguro).
5. Clique em **OK**.

Bate-papo na janela do Privacy Manager Chat

Depois de inicializar o Privacy Manager Chat, uma janela do Private Manager Chat é aberta no Windows Live Messenger. Utilizar o Privacy Manager Chat é similar a utilizar o Windows Live Messenger básico, a não ser pelos seguintes recursos adicionais que estão disponíveis na janela Privacy Manager Chat:

- **Save** (Salvar) — Clique neste botão para salvar a sua sessão de bate-papo na pasta especificada nas suas definições de configuração. Você também pode configurar o Privacy Manager Chat para salvar automaticamente cada sessão quando é fechado.
- **Hide all** (Ocultar Tudo) e **Show all** (Exibir Tudo) — Clique no botão apropriado para expandir ou ocultar as mensagens mostradas na janela Secure Communications (Comunicação Segura). Você também pode ocultar ou exibir mensagens clicando no cabeçalho da mensagem.
- **Are you there?** (Você está aí?) — Clique neste botão para solicitar autenticação por parte do seu contato.
- **Lock** (Bloquear) — Clique neste botão para fechar a janela Privacy Manager Chat e voltar à janela Chat Entry (Entrada de Bate-papo). Para exibir novamente a janela Secure Communications (Comunicação Segura), clique em **Resume the session** (Retomar a sessão) e depois autentique utilizando o método de login de segurança da sua escolha.
- **Send** (Enviar) — Clique neste botão para enviar uma mensagem criptografada ao seu contato.
- **Send signed** (Envio com assinatura) — Selecione esta caixa de seleção para assinar e criptografar eletronicamente suas mensagens. Então, se a mensagem for adulterada, será marcada como inválida quando for recebida pelo destinatário. Você precisa autenticar toda vez que envia uma mensagem assinada.
- **Send hidden** (Envio oculto) — Selecione esta caixa de seleção para criptografar e enviar uma mensagem exibindo apenas o cabeçalho da mensagem. O seu contato precisa realizar a autenticação para ler o conteúdo da mensagem.

Visualização do histórico de bate-papo

O Privacy Manager Chat History Viewer (Visualizador de Histórico do Privacy Manager Chat) exibe arquivos de sessão criptografados do Privacy Manager Chat. As sessões podem ser salvas clicando em Save (Salvar) na janela Privacy Manager Chat, ou configurando o salvamento automático na guia Chat (Bate-papo) no Privacy Manager. No visualizador, cada sessão mostra o Contact Screen Name (Nome de Tela do Contato) (criptografado) e a data e hora em que a sessão começou e terminou. Como padrão, as sessões são exibidas para todas as contas de e-mail que você configurou. Você pode usar menu **Display history for** (Exibir histórico para) para selecionar apenas a visualização de contas específicas.

Inicialização do Chat History Viewer

1. Clique em **Iniciar**, **Todos os Programas** e **HP ProtectTools Security Manager**.
2. Clique em **Privacy Manager: Sign and Chat** e depois clique em **Chat History Viewer** (Visualizador do Histórico de Bate-papo).

– ou –

▲ Em uma sessão de bate-papo, clique em **History Viewer** (Visualizador de Histórico) ou em **History** (Histórico).

– ou –

▲ Na página “Chat Configuration” (Configuração de Bate-papo), clique em **Start Live Messenger History Viewer** (Iniciar Visualizador de Histórico do Live Messenger).

Revelar todas as sessões

Revelar todas as sessões exibe o Contact Screen Name (Nome de Tela do Contato) descriptografado para a sessão(ões) atualmente selecionada(s) e todas as sessões na mesma conta.

1. No Chat History Viewer (Visualizador de Histórico de Bate-papo), clique com o botão direito em qualquer sessão e depois selecione **Reveal All Sessions** (Revelar Todas as Sessões).
2. Faça a autenticação utilizando o método de login de segurança de sua escolha.

   Os Contact Screen Names (Nomes de Tela dos Contatos) são descriptografados.
3. Clique duas vezes em qualquer sessão para visualizar seu conteúdo.

Revelar sessões para uma conta específica

Revelar uma sessão exibe o Contact Screen Name (Nome de Tela do Contato) descriptografado para a sessão atualmente selecionada.

1. No Chat History Viewer (Visualizador de Histórico de Bate-papo), clique com o botão direito em qualquer sessão e depois selecione **Reveal Session** (Revelar Sessão).
2. Faça a autenticação utilizando o método de login de segurança de sua escolha.

   Os Contact Screen Names (Nomes de Tela dos Contatos) são descriptografados.
3. Clique duas vezes na sessão revelada para visualizar seu conteúdo.

NOTA: Sessões adicionais criptografadas com o mesmo certificado vão mostrar um ícone desbloqueado, indicando que você pode vê-las clicando duas vezes em qualquer uma dessas sessões sem autenticação adicional. Sessões criptografadas com um certificado diferente vão mostrar um ícone bloqueado, indicando que uma autenticação adicional é necessária para essas sessões para essas sessões antes de exibir os Contact Screen Names (Nomes de Tela dos Contatos) ou o conteúdo.

Visualização de uma ID de sessão

▲ No Chat History View (Visualizador de Histórico de Bate-papo), clique com o botão direito em qualquer sessão revelada e selecione **View session ID** (Visualizar ID de sessão).

Visualização de uma sessão

Visualizar uma sessão abre o arquivo para visualização. Se a sessão não foi revelada — exibindo o Contact Screen Name (Nome de Tela do Contato) descriptografado — anteriormente, ela é revelada ao mesmo tempo.

1. No Chat History Viewer (Visualizador de Histórico de Bate-papo), clique com o botão direito em qualquer sessão revelada e selecione **View** (Visualizar).
2. Se solicitado, faça a autenticação utilizando o método de login de segurança de sua escolha.

O conteúdo da sessão é descriptografado.

Busca de um texto específico nas sessões

Você só pode buscar texto em sessões reveladas (descriptografadas) que são exibidas na janela do visualizador. Estas são as sessões onde o Contact Screen Name (Nome de Contato de Tela) é mostrado em texto simples.

1. No Chat History Viewer (Visualizador de Histórico de Bate-papo), clique no botão **Search** (Procurar).
2. Digite o texto da busca, configure qualquer parâmetro de busca desejado e depois clique em **OK**.

   Sessões que contêm o texto são realçadas na janela do visualizador.

Exclusão de uma sessão

1. Selecione uma sessão de histórico de bate-papo.
2. Clique em **Delete** (Excluir).

Adição ou remoção de colunas

Como padrão, as 3 colunas mais utilizadas são exibidas no Chat History Viewer. Você pode acrescentar colunas adicionais à exibição ou remover colunas da exibição.

Para acrescentar colunas à exibição:

1. Clique com o botão direito em qualquer cabeçalho de coluna e selecione **Add/Remove Columns** (Adicionar/Remover Colunas).
2. Selecione um cabeçalho de coluna no painel esquerdo e depois clique em **Add** (Adicionar) para movê-lo para o painel direito.

Para remover colunas da exibição:

1. Clique com o botão direito em qualquer cabeçalho de coluna e selecione **Add/Remove Columns** (Adicionar/Remover Colunas).
2. Selecione um cabeçalho de coluna no painel direito e depois clique em **Remove** (Remover) para movê-lo para o painel esquerdo.

Filtragem de sessões exibidas

Uma lista de sessões para todas as suas contas é exibida no Chat History Viewer.

Exibição de sessões para uma conta específica

▲ No Chat History Viewer (Visualizador de Histórico de Bate-papo), selecione uma conta a partir do menu **Display history for** (Exibir histórico para).

Exibição de sessões para um intervalo de datas

1. No Chat History Viewer (Visualizador de Histórico de Bate-papo), clique no botão **Advanced Filter** (Filtro Avançado).

   A caixa de diálogo Advanced Filter (Filtro Avançado) é exibida.

2. Selecione a caixa de seleção **Display only sessions within specified date range** (Exibir apenas sessões dentro do intervalo de datas especificado).

3. Nas caixas **From date** (Data inicial) e **To date** (Data final), digite o dia, mês e/ou ano, ou clique na seta junto ao calendário para selecionar as datas.

4. Clique em **OK**.

Exibição de sessões salvas em uma pasta diferente da pasta padrão

1. No Chat History Viewer (Visualizador de Histórico de Bate-papo), clique no botão **Advanced Filter** (Filtro Avançado).

2. Selecione a caixa de seleção **Use an alternate history files folder** (Use uma pasta alternativa para arquivos de histórico)

3. Digite o local da pasta, ou clique em **Browse** (Procurar) para buscar uma pasta.

4. Clique em **OK**.

Tarefas avançadas

Migração de Certificados do Privacy Manager e contatos confiáveis para um computador diferente

Você pode migrar com segurança os seus Certificados do Privacy Manager e contatos confiáveis para um computador diferente. Para fazer isso, exporte-os como um arquivo protegido por senha para um local de rede ou para qualquer dispositivo de armazenamento removível e depois importe o arquivo para um novo computador.

Exportação de Privacy Manager Certificates (Certificados do Privacy Manager) e Trusted Contacts (Contatos Confiáveis)

Para exportar seus Privacy Manager Certificates (Certificados do Privacy Manager) e Trusted Contacts (Contatos Confiáveis) para um arquivo protegido por senha, siga estas etapas:

1. Abra o Privacy Manager e clique em **Migration** (Migração).
2. Clique em **Export migration file** (Exportar arquivo de migração).
3. Na página “Select Data” (Selecionar Dados), selecione as categorias de dados a serem incluídas no arquivo de migração e depois clique em **Next** (Avançar).
4. Na página “Migration File” (Arquivo de Migração), digite um nome de arquivo ou clique em **Browse** (Pesquisar) para encontrar uma localização de arquivo e depois clique em **Next** (Avançar).
5. Insira e confirme uma senha e, em seguida, clique em **Next** (Avançar).

   NOTA: Armazene esta senha em um lugar seguro, porque vai precisar dela quando importar o arquivo de migração.

6. Faça a autenticação utilizando o método de login de segurança de sua escolha.
7. Na página “Migration File Saved” (Arquivo de Migração Salvo), clique em **Finish** (Concluir).

Importação de Privacy Manager Certificates (Certificados do Privacy Manager) e Trusted Contacts (Contatos Confiáveis)

Para importar seus Certificados do Privacy Manager e contatos confiáveis para um arquivo protegido por senha, siga estas etapas:

1. Abra o Privacy Manager e clique em **Migration** (Migração).
2. Clique em **Import migration file** (Importar arquivo de migração).
3. Na página “Select Data” (Selecionar Dados), selecione as categorias de dados a serem incluídas no arquivo de migração e depois clique em **Next** (Avançar).
4. Na página “Migration File” (Arquivo de Migração), digite um nome de arquivo ou clique em **Browse** (Pesquisar) para encontrar uma localização de arquivo e depois clique em **Next** (Avançar).
5. Na página “Migration File Import” (Importar Arquivo de Migração), clique em **Finish** (Concluir).

5 File Sanitizer for HP ProtectTools

O File Sanitizer é uma ferramenta que permite fragmentar com segurança ativos de dados (informações pessoais ou arquivos, dados de histórico ou relacionados à Web, ou outros componentes de dados) do computador e periodicamente limpar sua unidade de disco rígido.

NOTA: O File Sanitizer opera somente no disco rígido.

Sobre fragmentação

Excluir um ativo no Windows não remove completamente o conteúdo desse ativo do seu disco rígido. O Windows exclui somente a referência ao ativo. O conteúdo do ativo permanece no disco rígido até que outro ativo sobrescreva essa mesma área no disco rígido com novas informações.

A fragmentação é diferente de uma exclusão padrão do Windows® (também conhecida como exclusão simples no File Sanitizer) na qual quando você fragmenta um ativo, um algoritmo que oculta os dados é invocado, o que torna praticamente impossível recuperar o ativo original.

Quando se escolhe um arquivo fragmentado (Segurança alta, Segurança média ou Segurança baixa), uma lista predefinida de ativos e um método de apagamento são automaticamente selecionados para a fragmentação. Também é possível personalizar um perfil de fragmentação, o que permite especificar o número de ciclos de fragmentação, quais ativos incluir na fragmentação, quais ativos confirmar antes da fragmentação e quais ativos excluir da fragmentação.

É possível configurar uma programação de fragmentação automática, além de fragmentar manualmente os ativos sempre que desejado.

A limpeza de espaço livre permite gravar com segurança dados aleatórios sobre os ativos excluídos, evitando que os usuários visualizem os conteúdos originais do ativo excluído.

Sobre limpeza de espaço livre

NOTA: A limpeza de espaço livre é para os ativos que você exclui utilizando a Lixeira do Windows ou manualmente. A limpeza de espaço livre não oferece segurança adicional aos ativos fragmentados.

Você pode definir uma programação de limpeza de espaço livre automática ou pode ativar manualmente essa limpeza usando o ícone HP ProtectTools na área de notificação, à direita da barra de tarefas.

Procedimentos de configuração

Abertura do File Sanitizer

Para abrir o File Sanitizer:

1. Clique em **Iniciar**, **Todos os Programas** e **HP ProtectTools Security Manager**.
2. Clique em **File Sanitizer**.

   – ou –

- Clique duas vezes no ícone **File Sanitizer**.

  – ou –

- Clique com o botão direito no ícone do HP ProtectTools na área de notificação, à direita da barra de tarefas, clique em File Sanitizer e, em seguida, clique em Open File Sanitizer (Abrir File Sanitizer).

Configuração de uma programação de fragmentação

1. Abra o File Sanitizer e clique em **Shred** (Fragmentar).
2. Selecione uma opção de fragmentação:
   - **Windows startup** (Ao iniciar o Windows) — Escolha esta opção para fragmentar todos os ativos selecionados quando o Windows iniciar.
   - **Windows shutdown** (Ao desligar o Windows) — Escolha esta opção para fragmentar todos os ativos selecionados quando o Windows desligar.

     NOTA: Quando esta opção for selecionada, uma caixa de diálogo será exibida no desligamento, perguntando se deseja continuar com a fragmentação dos ativos selecionados ou se deseja ignorar o procedimento. Clique em **Yes** (Sim) para ignorar o procedimento de fragmentação ou em **No** (Não) para continuar a fragmentação.

   - **Web browser open** (Ao abrir o navegador da Web) — Escolha esta opção para fragmentar todos os ativos relacionados à Web selecionados, como um Histórico de URL do navegador, quando você abrir o navegador da Web.
   - **Web browser quit** (Ao sair do navegador da Web) — Escolha esta opção para fragmentar todos os ativos relacionados à Web selecionados, como um histórico de URL do navegador, quando você fechar um navegador da Web.
   - **Scheduler** (Programador) — Marque a caixa de verificação Activate Scheduler (Ativar Programador), insira sua senha do Windows e, em seguida, insira o dia e a hora para fragmentar os ativos selecionados.
3. Clique em **Apply** (Aplicar) e em **OK**.

Configuração de uma programação de limpeza de espaço livre

NOTA: A limpeza de espaço livre é para os ativos que você exclui utilizando a Lixeira do Windows ou manualmente. A limpeza de espaço livre não oferece segurança adicional aos ativos fragmentados.

Para configurar uma programação de limpeza de espaço livre:

1. Abra o File Sanitizer e clique em **Free Space Bleaching** (Limpeza de espaço livre).
2. Marque a caixa de diálogo **Activate Scheduler** (Ativar agendador), digite sua senha do Windows e, em seguida, o dia e a hora para executar a limpeza do disco rígido.
3. Clique em **Apply** (Aplicar) e em **OK**.

   NOTA: A operação de limpeza de espaço livre pode demorar bastante. Mesmo que a limpeza de espaço livre seja executada no fundo, seu computador pode ter a capacidade reduzida pelo aumento no uso do processador.

Seleção ou criação de um perfil de fragmentação

Você pode especificar um método para apagar e selecionar os ativos para fragmentação selecionando um perfil predefinido ou criando seu próprio perfil.

Seleção de um perfil de fragmentação predefinido

Quando se escolhe um perfil de fragmentação predefinido (Alta segurança, Média segurança ou Baixa segurança), um método de exclusão e uma lista de ativos predefinidos são automaticamente selecionados. Clique no botão View Details (Exibir detalhes) para exibir a lista predefinida de ativos que estão selecionados para fragmentação.

Para selecionar um perfil de fragmentação predefinido:

1. Abra o **File Sanitizer** e clique em **Settings** (Configurações).
2. Clique em um perfil de fragmentação predefinido.
3. Clique em **View Details** (Exibir detalhes) para exibir a lista de ativos que estão selecionados para fragmentação.
4. Em **Shred the following** (Fragmentar o seguinte), marque a caixa de seleção de cada ativo que você deseja confirmar antes da fragmentação.
5. Clique em **Cancel** (Cancelar) e em **OK**.

Personalização de um perfil de fragmentação

Ao criar um perfil de fragmentação, especifique o número de ciclos de fragmentação, quais ativos incluir na fragmentação, quais ativos confirmar antes da fragmentação e quais ativos excluir da fragmentação:

1. Abra o File Sanitizer, clique em **Settings** (Configurações), em **Advanced Security Settings** (Configurações de segurança avançadas) e, em seguida, clique em **View Details** (Exibir detalhes).

2. Especifique o número de ciclos de fragmentação.

   NOTA: O número selecionado de ciclos de fragmentação será executado para cada ativo. Por exemplo, se você escolher três ciclos de fragmentação, um algoritmo que oculta os dados será executado três vezes. Se você escolher ciclos de fragmentação de alta segurança, a fragmentação talvez demore bastante; porém, quanto maior o número de ciclos de fragmentação especificado, mais seguro estará o computador.

3. Selecione os ativos que deseja fragmentar:

   a. Em **Available shred options** (Opções de fragmentação disponíveis), clique em um ativo e em **Add** (Adicionar).

   b. Para adicionar um ativo personalizado, clique em Add Custom Option (Adicionar opção personalizada), digite um nome de arquivo ou nome de pasta e clique em **OK**. Clique no ativo personalizado e, em seguida, clique em **Add** (Adicionar).

      NOTA: Para excluir um ativo das opções de fragmentação disponíveis, clique no ativo e, em seguida, clique em **Delete** (Excluir).

4. Em **Shred the following** (Fragmentar o seguinte), marque a caixa de seleção de cada ativo que você deseja confirmar antes da fragmentação.

   NOTA: Para remover um ativo da lista de fragmentação, clique no ativo e, em seguida, clique em **Remove** (Remover).

5. Em **Do not shred the following** (Não fragmentar o seguinte), clique em **Add** (Adicionar) para selecionar os ativos específicos que deseja excluir da fragmentação.

   NOTA: Somente extensões de arquivo podem ser excluídas da fragmentação. Por exemplo, se você adicionar a extensão de arquivo .BMP, todos os arquivos com a extensão .BMP serão excluídos da fragmentação.

   Para remover um ativo da lista de extensões, clique no ativo e, em seguida, clique em **Delete** (Excluir).

6. Quando terminar de configurar o perfil de fragmentação, clique em **Apply** (Aplicar) e em **OK**.

Personalização de um perfil de exclusão simples

O perfil de exclusão simples executa a exclusão de um ativo padrão sem fragmentação. Ao personalizar um perfil de exclusão simples, especifique quais ativos incluir na exclusão simples, quais ativos confirmar antes que uma exclusão simples seja executada e quais ativos excluir da exclusão simples:

NOTA: É altamente recomendável que você execute uma limpeza de espaço livre regularmente se utilizar a opção de exclusão simples.

1. Abra o **File Sanitizer**, clique em **Settings** (Configurações), **Simple Delete Setting** (Configuração de exclusão simples) e, em seguida, clique em **View Details** (Exibir detalhes).
2. Selecione os ativos que deseja excluir:
   a. Em **Available delete options** (Opções de exclusão disponíveis), clique no ativo e, em seguida, clique em **Add** (Adicionar).
   b. Para adicionar um ativo personalizado, clique em **Add Custom Option** (Adicionar opção personalizada), digite um nome de arquivo ou nome de pasta e clique em **OK**. Clique no ativo personalizado e, em seguida, clique em **Add** (Adicionar).

   NOTA: Para excluir um ativo das opções de exclusão disponíveis, clique no ativo e, em seguida, clique em **Delete** (Excluir).
3. Em **Delete the following** (Excluir o seguinte), marque a caixa de seleção de cada ativo que você deseja confirmar antes da exclusão.

   NOTA: Para remover um ativo da lista de exclusão, clique no ativo e, em seguida, clique em **Remove** (Remover).
4. Em **Do not shred the following** (Não fragmentar o seguinte), clique em **Add** (Adicionar) para selecionar os ativos específicos que deseja excluir da fragmentação.

   NOTA: Somente extensões de arquivo podem ser excluídas da exclusão. Por exemplo, se você adicionar a extensão de arquivo .BMP, todos os arquivos com a extensão .BMP serão excluídos da exclusão.

   Para remover um ativo da lista de extensões, clique no ativo e, em seguida, clique em **Delete** (Excluir).
5. Quando terminar de configurar o perfil de exclusão simples, clique em **Apply** (Aplicar) e em **OK**.

Configuração de uma programação de fragmentação

1. Abra o File Sanitizer e clique em **Shred** (Fragmentar).
2. Selecione uma opção de fragmentação:
   - **Windows startup** (Ao iniciar o Windows) — Escolha esta opção para fragmentar todos os ativos selecionados quando o Windows iniciar.
   - **Windows shutdown** (Ao desligar o Windows) — Escolha esta opção para fragmentar todos os ativos selecionados quando o Windows desligar.

     NOTA: Quando esta opção for selecionada, uma caixa de diálogo será exibida no desligamento, perguntando se deseja continuar com a fragmentação dos ativos selecionados ou se deseja ignorar o procedimento. Clique em Yes (Sim) para ignorar o procedimento de fragmentação ou No (Não) para continuar a fragmentação.
   - **Web browser open** (Ao abrir o navegador da Web) — Escolha esta opção para fragmentar todos os ativos relacionados à Web selecionados, como um Histórico de URL do navegador, quando você abrir o navegador da Web.

- **Web browser quit** (Ao sair do navegador da Web) — Escolha esta opção para fragmentar todos os ativos relacionados à Web selecionados, como um histórico de URL do navegador, quando você fechar um navegador da Web.

- **Scheduler** (Programador) — Marque a caixa de verificação Activate Scheduler (Ativar Programador), insira sua senha do Windows e, em seguida, insira o dia e a hora para fragmentar os ativos selecionados.

3. Clique em **Apply** (Aplicar) e em **OK**.

Configuração de uma programação de limpeza de espaço livre

NOTA: A limpeza de espaço livre é para os ativos que você exclui utilizando a Lixeira do Windows ou manualmente. A limpeza de espaço livre não oferece segurança adicional aos ativos fragmentados.

Para configurar uma programação de limpeza de espaço livre:

1. Abra o File Sanitizer e clique em **Free Space Bleaching** (Limpeza de espaço livre).

2. Marque a caixa de diálogo **Activate Scheduler** (Ativar agendador), digite sua senha do Windows e, em seguida, o dia e a hora para executar a limpeza do disco rígido.

3. Clique em **Apply** (Aplicar) e em **OK**.

   NOTA: A operação de limpeza de espaço livre pode demorar bastante. Mesmo que a limpeza de espaço livre seja executada no fundo, seu computador pode ter a capacidade reduzida pelo aumento no uso do processador.

Seleção ou criação de um perfil de fragmentação

Seleção de um perfil de fragmentação predefinido

Quando se escolhe um perfil de fragmentação predefinido (Alta segurança, Média segurança ou Baixa segurança), um método de exclusão e uma lista de ativos predefinidos são automaticamente selecionados. Clique no botão View Details (Exibir detalhes) para exibir a lista predefinida de ativos que estão selecionados para fragmentação.

Para selecionar um perfil de fragmentação predefinido:

1. Abra o **File Sanitizer** e clique em **Settings** (Configurações).

2. Clique em um perfil de fragmentação predefinido.

3. Clique em **View Details** (Exibir detalhes) para exibir a lista de ativos que estão selecionados para fragmentação.

4. Em **Shred the following** (Fragmentar o seguinte), marque a caixa de seleção de cada ativo que você deseja confirmar antes da fragmentação.

5. Clique em **Cancel** (Cancelar) e em **OK**.

Personalização de um perfil de fragmentação

Ao criar um perfil de fragmentação, especifique o número de ciclos de fragmentação, quais ativos incluir na fragmentação, quais ativos confirmar antes da fragmentação e quais ativos excluir da fragmentação:

1. Abra o File Sanitizer, clique em **Settings** (Configurações), em **Advanced Security Settings** (Configurações de segurança avançadas) e, em seguida, clique em **View Details** (Exibir detalhes).

2. Especifique o número de ciclos de fragmentação.

   NOTA: O número selecionado de ciclos de fragmentação será executado para cada ativo. Por exemplo, se você escolher três ciclos de fragmentação, um algoritmo que oculta os dados será executado três vezes. Se você escolher ciclos de fragmentação de alta segurança, a fragmentação talvez demore bastante; porém, quanto maior o número de ciclos de fragmentação especificado, mais seguro estará o computador.

3. Selecione os ativos que deseja fragmentar:

   a. Em **Available shred options** (Opções de fragmentação disponíveis), clique em um ativo e em **Add** (Adicionar).

   b. Para adicionar um ativo personalizado, clique em Add Custom Option (Adicionar opção personalizada), digite um nome de arquivo ou nome de pasta e clique em **OK**. Clique no ativo personalizado e, em seguida, clique em **Add** (Adicionar).

      NOTA: Para excluir um ativo das opções de fragmentação disponíveis, clique no ativo e, em seguida, clique em **Delete** (Excluir).

4. Em **Shred the following** (Fragmentar o seguinte), marque a caixa de seleção de cada ativo que você deseja confirmar antes da fragmentação.

   NOTA: Para remover um ativo da lista de fragmentação, clique no ativo e, em seguida, clique em **Remove** (Remover).

5. Em **Do not shred the following** (Não fragmentar o seguinte), clique em **Add** (Adicionar) para selecionar os ativos específicos que deseja excluir da fragmentação.

   NOTA: Somente extensões de arquivo podem ser excluídas da fragmentação. Por exemplo, se você adicionar a extensão de arquivo .BMP, todos os arquivos com a extensão .BMP serão excluídos da fragmentação.

   Para remover um ativo da lista de extensões, clique no ativo e, em seguida, clique em **Delete** (Excluir).

6. Quando terminar de configurar o perfil de fragmentação, clique em **Apply** (Aplicar) e em **OK**.

Personalização de um perfil de exclusão simples

O perfil de exclusão simples executa a exclusão de um ativo padrão sem fragmentação. Ao personalizar um perfil de exclusão simples, especifique quais ativos incluir na exclusão simples, quais ativos confirmar antes que uma exclusão simples seja executada e quais ativos excluir da exclusão simples:

NOTA: É altamente recomendável que você execute uma limpeza de espaço livre regularmente se utilizar a opção de exclusão simples.

1. Abra o **File Sanitizer**, clique em **Settings** (Configurações), **Simple Delete Setting** (Configuração de exclusão simples) e, em seguida, clique em **View Details** (Exibir detalhes).
2. Selecione os ativos que deseja excluir:
   - Em **Available delete options** (Opções de exclusão disponíveis), clique no ativo e, em seguida, clique em **Add** (Adicionar).
   - Para adicionar um ativo personalizado, clique em **Add Custom Option** (Adicionar opção personalizada), digite um nome de arquivo ou nome de pasta e clique em **OK**. Clique no ativo personalizado e, em seguida, clique em **Add** (Adicionar).

   NOTA: Para excluir um ativo das opções de exclusão disponíveis, clique no ativo e, em seguida, clique em **Delete** (Excluir).
3. Em **Delete the following** (Excluir o seguinte), marque a caixa de seleção de cada ativo que você deseja confirmar antes da exclusão.

   NOTA: Para remover um ativo da lista de exclusão, clique no ativo e, em seguida, clique em **Remove** (Remover).
4. Em **Do not delete the following** (Não excluir o seguinte), clique em **Add** (Adicionar) para selecionar os ativos específicos que deseja excluir da fragmentação.

   NOTA: Somente extensões de arquivo podem ser excluídas da exclusão. Por exemplo, se você adicionar a extensão de arquivo .BMP, todos os arquivos com a extensão .BMP serão excluídos da exclusão.

   Para remover um ativo da lista de extensões, clique no ativo e, em seguida, clique em **Delete** (Excluir).
5. Quando terminar de configurar o perfil de exclusão simples, clique em **Apply** (Aplicar) e em **OK**.

Tarefas básicas

Uso de uma seqüência de teclas para iniciar a fragmentação

Para especificar uma seqüência de teclas, siga estas etapas:

1. Abra o **File Sanitizer** e clique em **Shred** (Fragmentar).
2. Marque a caixa de seleção **Key sequence** (Seqüência de teclas).
3. Digite um caractere na caixa disponível e marque a caixa **CTRL**, **ALT** ou **SHIFT**, ou selecione todas as três opções.

   Por exemplo, para iniciar a fragmentação automática usando a tecla s e ctrl+shift, digite s na caixa e, em seguida, marque as opções **CTRL** e **SHIFT**.

   NOTA: Certifique-se de selecionar uma seqüência de teclas diferente das outras seqüências de teclas que você configurou.

Para iniciar a fragmentação usando uma seqüência de teclas:

1. Mantenha pressionada a tecla ctrl, alt ou shift (ou qualquer outra combinação especificada) enquanto pressiona o caractere escolhido.
2. Se a caixa de diálogo de confirmação for exibida, clique em **Yes** (Sim).

Uso do ícone do File Sanitizer

CUIDADO: Ativos fragmentados não podem ser recuperados. Considere cuidadosamente quais itens selecionar para uma fragmentação manual.

1. Navegue até o documento ou pasta que deseja fragmentar.
2. Arraste o ativo para o ícone do File Sanitizer na área de trabalho.
3. Quando a caixa de diálogo de confirmação for exibida, clique em **Yes** (Sim).

Fragmentação manual de um ativo

CUIDADO: Ativos fragmentados não podem ser recuperados. Considere cuidadosamente quais itens selecionar para uma fragmentação manual.

1. Clique com o botão direito no ícone do **HP ProtectTools** na área de notificação, à direita da barra de tarefas, clique em **File Sanitizer** e, depois, em **Shred One** (Fragmentar um).
2. Quando a caixa de diálogo Procurar for exibida, navegue até o ativo que deseja fragmentar e clique em **OK**.

   NOTA: O ativo selecionado pode ser um único arquivo ou pasta.

3. Quando a caixa de diálogo de confirmação for exibida, clique em **Yes** (Sim).

– ou –

1. Clique com o botão direito no ícone do **File Sanitizer** na área de trabalho e, em seguida, clique em **Shred One** (Fragmentar um).
2. Quando a caixa de diálogo Procurar for exibida, navegue até o ativo que deseja fragmentar e clique em **OK**.
3. Quando a caixa de diálogo de confirmação for exibida, clique em **Yes** (Sim).

– ou –

1. Abra o File Sanitizer e clique em **Shred** (Fragmentar).
2. Clique no botão **Browse** (Procurar).
3. Quando a caixa de diálogo Procurar for exibida, navegue até o ativo que deseja fragmentar e clique em **OK**.
4. Quando a caixa de diálogo de confirmação for exibida, clique em **Yes** (Sim).

– ou –

1. Abra o File Sanitizer e clique em **Shred** (Fragmentar).
2. Clique no botão **Shred Now** (Fragmentar agora).
3. Quando a caixa de diálogo de confirmação for exibida, clique em **Yes** (Sim).

Fragmentação manual de todos os arquivos selecionados

1. Clique com o botão direito no ícone do **HP ProtectTools** na área de notificação, à direita da barra de tarefas, clique em **File Sanitizer** e, depois, em **Shred Now** (Fragmentar agora).
2. Quando a caixa de diálogo de confirmação for exibida, clique em **Yes** (Sim).

   – ou –

1. Clique com o botão direito no ícone do **File Sanitizer** na área de trabalho e, em seguida, clique em **Shred Now** (Fragmentar agora).
2. Quando a caixa de diálogo de confirmação for exibida, clique em **Yes** (Sim).

Ativação manual da limpeza de espaço livre

1. Clique com o botão direito no ícone do **HP ProtectTools** na área de notificação, à direita da barra de tarefas, clique em **File Sanitizer** e, depois, em **Bleach Now** (Limpar agora).
2. Quando a caixa de diálogo de confirmação for exibida, clique em **Yes** (Sim).

– ou –

1. Abra o File Sanitizer e clique em **Free Space Bleaching** (Limpeza de espaço livre).
2. Clique em **Bleach Now** (Limpar agora).
3. Quando a caixa de diálogo de confirmação for exibida, clique em **Yes** (Sim).

Interrupção de uma operação de fragmentação ou de limpeza de espaço livre

Quando uma operação de fragmentação ou de limpeza de espaço livre está em andamento, uma mensagem é exibida acima do ícone do HP ProtectTools Security Manager, na área de notificação. A mensagem fornece detalhes sobre o processo de fragmentação ou de limpeza de espaço livre (porcentagem completa) e oferece a opção de interromper a operação.

Para interromper a operação:

▲ Clique na mensagem e, em seguida, clique em **Stop** (Parar) para cancelar a operação.

Exibição dos arquivos de registro

Toda vez que uma operação de fragmentação ou limpeza de espaço livre é executada, são gerados arquivos de registro de erros e falhas. Os arquivos de registro são sempre atualizados de acordo com a última operação de fragmentação ou limpeza de espaço livre.

NOTA: Os arquivos cuja fragmentação ou limpeza tenha sido bem-sucedida não são exibidos nos arquivos de registro.

Um arquivo de registro é criado para operações de fragmentação e outro para operações de limpeza de espaço livre. Ambos os arquivos de registro estão localizados no disco rígido em:

- C:\Arquivos de programas\Hewlett-Packard\File Sanitizer\`[Nome_de_usuário]`_ShredderLog.txt
- C:\Arquivos de programas\Hewlett-Packard\File Sanitizer\`[Nome_de_usuário]`_DiskBleachLog.txt

6 BIOS Configuration for HP ProtectTools

O oferece o acesso às configurações de segurança e configuração do utilitário de configuração. Isso dá aos usuários Windows o acesso aos recursos de segurança do sistema que são gerenciados pelo utilitário de configuração.

Com o BIOS Configuration, é possível executar os seguintes objetivos:

- Gerenciar senhas de administrador.
- Configurar outros recursos de autenticação na inicialização, tais como autenticação da segurança integrada.
- Ativar e desativar recursos de hardware, como a inicialização via CD-ROM ou portas de hardware.
- Configurar opções de inicialização que incluem ativar a inicialização múltipla e alterar a ordem de inicialização.

NOTA: A maioria dos recursos de também estão disponíveis no utilitário de configuração.

Tarefas básicas

O BIOS Configuration permite o gerenciamento de várias configurações do computador que, de outra forma, somente seriam acessíveis pressionando f10 na inicialização para entrar no utilitário de configuração do computador.

Acesso ao BIOS Configuration

Para acessar o BIOS Configuration:

1. Clique em **Iniciar**, **Configurações** e, em seguida, clique em **Painel de Controle**.
2. Clique em **HP ProtectTools Security Manager**, em seguida clique em **BIOS Configuration**.

   Também é possível acessar o BIOS Configuration a partir de um ícone na área de notificação, no lado direito da barra de tarefas.

   NOTA: Para exibir o ícone do HP ProtectTools Security Manager, talvez seja necessário clicar no ícone **Mostrar ícones ocultos** (**<** ou **<<**) na área de notificação.

   - Clique com o botão direito no ícone **HP ProtectTools Security Manager**, localizado na área de notificação.
   - Clique em **BIOS Configuration**.
3. Se for um usuário do HP ProtectTools, insira sua senha do Windows.
   - Se você informar a senha do Windows corretamente, mas não for um administrador do BIOS, sua capacidade de efetuar alterações variará dependendo das configurações de nível de segurança. Consulte Definição de opções de configuração do sistema na página 70

     NOTA: Um usuário do HP ProtectTools pode ser ou não um administrador do BIOS.
   - Se informar a senha do Windows incorretamente, você poderá visualizar as configurações do BIOS Configuration, mas não poderá alterá-las.
4. Se você não for um usuário do HP ProtectTools, o software BIOS Configuration verificará se uma senha de administrador do BIOS foi definida.
   - Se uma senha de administrador do BIOS tiver sido definida, você precisará informá-la.
     - Se informar a senha de administrador do BIOS corretamente, você poderá visualizar e alterar as configurações do BIOS Configuration.
     - Se uma senha de administrador do BIOS tiver sido definida e você não a informar ou informá-la incorretamente, você poderá visualizar as configurações do BIOS Configuration, mas não poderá alterá-las.
   - Se uma senha de administrador do BIOS não tiver sido definida, você poderá visualizar e alterar as configurações do BIOS Configuration.

Visualização ou alteração das configurações

Para visualizar ou alterar opções de configuração:

1. Clique em uma das páginas do BIOS Configuration:
   - File (Arquivo)
   - Security (Segurança)
   - System Configuration (Configuração do Sistema)
2. Faça suas alterações e clique em **Apply** (Aplicar) para salvá-las e deixar a janela aberta.

   – ou –

   Faça suas alterações e clique em **OK** para salvá-las e fechar a janela.
3. Saia e reinicie o computador.

   Suas alterações entram em vigor quando o computador reinicia.

NOTA: As alterações de senha entram em vigor imediatamente, sem que seja necessário reiniciar o computador.

Exibição de informações do sistema

Use a página “File” (Arquivo) para visualizar os seguintes tipos de informação:

- Informações de identificação sobre o computador (incluindo número de série) e sobre as baterias no sistema
- Informações de especificação sobre o processador, o tamanho da memória e do cache, a revisão do vídeo, a versão da controladora do teclado e a ROM do sistema

NOTA: A página “File” (Arquivo) é somente para fins de informação. Nenhuma das informações exibidas pode ser modificada.

Para visualizar informações do sistema:

▲ Acesse o BIOS Configuration e clique em **File** (Arquivo).

Tarefas avançadas

Configuração de opções de segurança

Use a página “Security” (Segurança) do BIOS Configuration para aumentar a segurança do seu computador.

NOTA: Nem todas as opções estão disponíveis em todos os computadores, e opções adicionais também podem estar incluídas.

Para definir opções de segurança:

1. Acesse o BIOS Configuration e clique em **Security** (Segurança).
2. Selecione qualquer uma das opções listadas na tabela a seguir.
3. Altere as configurações conforme necessário.
4. Clique em **Apply** (Aplicar) para aplicar as novas configurações e deixar a janela aberta.

   – ou –

   Clique em **OK** para aplicar as novas configurações e fechar a janela.

Security (Segurança)

Opção	Ação
BIOS Administrator Password (Senha de administrador do BIOS) **NOTA:** Esta opção talvez seja denominada “Setup Password” (Senha de configuração).	Clique no botão **Set** (Definir) para definir uma senha de administrador do BIOS.

System IDs (IDs do sistema)

Opção	Ação
Ownership Tag (Etiqueta de propriedade)	Inserir, visualizar ou alterar.
Asset Tracking Number (Número de controle de ativo)	Inserir, visualizar ou alterar.

TPM Embedded Security

NOTA: Esse recurso é suportado somente em computadores equipados com HP ProtectTools Embedded Security Chip (TPM).

Opção	Ação
Reset of TPM from OS (Reinicialização do TPM a partir do SO)	Ativar ou desativar.
OS Management of TPM (Gerenciamento do TPM pelo SO)	Ativar ou desativar.
Embedded Security Device Availability (Disponibilidade de dispositivos do Embedded Security)	Selecionar disponível ou oculto.

Opção	Ação
Power-On Authentication Support (Suporte a autenticação na inicialização)	Ativar ou desativar o suporte de autenticação na inicialização por smart card. **NOTA:** Este recurso é suportado somente em computadores com leitores de smart card opcionais.
Automatic Drivelock Suppor (Suporte a Drivelock Automático)	Ativar ou desativar.

Administrator Tools (Ferramentas do administrador)

Opção	Ação
HP SpareKey	Ativar ou desativar.
Fingerprint Reset on Reboot (Restauração da impressão digital na reinicialização) (se existente)	Ativar ou desativar.

Password Policy (Política de senhas)

Opção	Ação
At least one symbol required (É necessário ao menos um símbolo)	Ativar ou desativar.
At least one number required (É necessário ao menos um número)	Ativar ou desativar.
At least one upper case character required (É necessário ao menos um caractere em letra maiúscula)	Ativar ou desativar.
At least one lower case character required (É necessário ao menos um caractere em letra minúscula)	Ativar ou desativar.
Are spaces allowed in password (Espaços são permitidos na senha)	Ativar ou desativar.

Hard Disk Sanitization Report (Relatório de limpeza do disco rígido)

Opção	Ação
Hard Disk Sanitization (Limpeza do disco rígido)	Se a limpeza do disco rígido tiver sido executada pelo menos uma vez, você poderá visualizar informações sobre os procedimentos de limpeza de disco mais recentes concluídos no computador. **NOTA:** Essa opção apaga dados sensíveis de uma unidade de disco rígido do computador. Se uma unidade de disco rígido tiver sido limpa e em seguida removida do computador, a informação sobre esse processo de limpeza ainda estará disponível.

Definição de opções de configuração do sistema

Use a página “System Configuration” (Configuração do Sistema) para visualizar e modificar opções de configuração do sistema.

NOTA: Nem todas as opções estão disponíveis em todos os computadores, e opções adicionais também podem estar incluídas.

Para definir opções de configuração do sistema:

1. Acesse **BIOS Configuration** e, em seguida, clique em **System Configuration** (Configuração do Sistema).
2. Selecione uma das opções a seguir, conforme descrito na tabela abaixo:
   - **Port option (Opções de porta)**
   - **Boot options (Opções de inicialização)**
   - **Device configuration options (Opções de configuração do dispositivo)**
   - **Built-in device options (Opções de dispositivo integrado)**
   - **AMT options (Opções AMT) (somente em determinados modelos)**
   - **Security level options (Opções de nível de segurança)**
3. Altere as configurações conforme necessário.
4. Clique em **Apply** (Aplicar) para aplicar as novas configurações ao sistema e deixar a janela aberta.

   – ou –

   Clique em **OK** na janela HP ProtectTools Security Manager para aplicar as novas configurações ao sistema e fechar a janela.

Port option (Opções de porta)

Opção	Ação
Flash Media Reader (Leitor de mídia flash)	Ativar ou desativar.
USB Ports (Portas USB)	Ativar ou desativar.
1394 port (Porta 1394)	Ativar ou desativar.
Express Card slot (Slot para Express Card)	Ativar ou desativar.

Boot options (Opções de inicialização)

Opção	Ação
Startup Check Delay (Sec) (Intervalo de espera da verificação de inicialização [seg.])	Definir o intervalo de espera da verificação de inicialização em segundos.
Custom Logo (Logotipo personalizado)	Ativar ou desativar.
Express Boot Popup Delay (Sec) (Intervalo de espera do pop-up do Express Boot [seg.])	Definir o intervalo de espera do pop-up do Express Boot em segundos.

Opção	Ação
CD-ROM Boot (Inicialização por CD-ROM)	Ativar ou desativar.
SD Card Boot (Inicialização por cartão SD)	Ativar ou desativar.
Boot from EFI File (Inicialização por arquivo EFI)	Ativar ou desativar.
Floppy boot (Inicialização por disquete)	Ativar ou desativar.
PXE Internal NIC boot (Inicialização por NIC interno PXE)	Ativar ou desativar.
Boot Order (Seqüência de inicialização)	Definir a seqüência na qual o sistema busca dispositivos para fazer a inicialização.

Device configuration options (Opções de configuração do dispositivo)

Opção	Ação
USB Legacy Support (Suporte de herança USB)	Ativar ou desativar.
Parallel port mode (Modo de porta paralela)	Selecionar um modo de porta paralela: padrão, bidirecional, EPP (Enhanced Parallel Port) ou ECP (Enhanced Capabilities Port).
Fan always on while on AC power (Ventilador sempre ligado quando houver alimentação de CA)	Ativar ou desativar o ventilador do sistema quando conectado a uma tomada de CA.
Data execution prevention (Prevenção da execução de dados)	Ativar/desativar a opção de monitorar o uso da memória e encerrar programas suspeitos.
SATA device mode (Modo de dispositivo SATA)	Selecionar IDE, AHCI ou RAID.
Dual core CPU (CPU Dual Core)	Ativar ou desativar.
Secondary battery fast charge (Carregamento rápido da bateria secundária)	Ativar ou desativar.
HP QuickLook 2	Ativar ou desativar.
TXT technology (Tecnologia TXT)	Ativar ou desativar.
Display Diagnostic URL (Exibir URL de diagnóstico)	Ativar ou desativar.
HDD Translation Mode (Modo de tradução do HD)	Selecionar Bit-shift (Deslocamento de bits) ou LBA-assisted (Assistência LBA).
Virtualization technology (Tecnologia de virtualização)	Ativar ou desativar a opção de permitir que várias máquinas virtuais executem lado a lado no mesmo computador.

Built-in device options (Opções de dispositivo integrado)

Opção	Ação
Wireless Button State (Estado do botão de conexão sem fio)	Ativar ou desativar.
Embedded WWAN Device Radio (Rádio de dispositivo WWAN integrado)	Ativar ou desativar.
Fingerprint Device (Dispositivo de impressão digital)	Ativar ou desativar.

Opção	Ação
Notebook MultiBay (MultiBay do notebook)	Ativar ou desativar.
Network Interface Controller (LAN) (Controlador de interface de rede [LAN])	Ativar ou desativar.
Ambient light sensor (Sensor de luz ambiente)	Ativar ou desativar.
Embedded Bluetooth® Device Radio (Rádio de dispositivo Bluetooth® integrado)	Ativar ou desativar.
Wake on LAN	Ativar ou desativar a opção de permitir ligar o computador remotamente a partir de um outro computador conectado à mesma rede.

AMT options (Opções AMT) (somente em determinados modelos)

Opção	Ação
Terminal Emulation Mode (Modo de emulação de terminal)	Selecionar ANSI ou VT100.
Firmware Verbosity (Verbosidade do firmware)	Ativar ou desativar.
Firmware Progress Event Support (Suporte a evento de progressão do firmware)	Ativar ou desativar.
Unconfigure AMT on next boot (Desconfigurar AMT na próxima inicialização)	Ativar ou desativar.

Security Level options (Opções de nível de segurança)

NOTA: Essas configurações controlam o nível de acesso dos usuários do HP ProtectTools.

Opção	Ação
CD-ROM Boot Security Level (Nível de segurança da inicialização por CD-ROM)	Alterar, visualizar ou ocultar.
Floppy Boot Security Level (Nível de segurança da inicialização por disquete)	Alterar, visualizar ou ocultar.
Internal Network Adapter Boot Security Level (Nível de segurança da inicialização por adaptador de rede interno)	Alterar, visualizar ou ocultar.
USB Legacy Support Security Level (Nível de segurança do suporte de herança USB)	Alterar, visualizar ou ocultar.
Fan Always on while on AC Power Security Level (Nível de segurança do ventilador sempre ligado quando houver alimentação de CA)	Alterar, visualizar ou ocultar.
Flash Media Reader Security Level (Nível de segurança do leitor de mídia flash)	Alterar, visualizar ou ocultar.
Startup Check Delay (Sec) Security Level (Nível de segurança do intervalo de espera da verificação da inicialização [seg.])	Alterar, visualizar ou ocultar.

Parallel Port Mode Security Level (Nível de segurança do modo de porta paralela)	Alterar, visualizar ou ocultar.
Express Boot Popup Delay (Sec) Security Level (Nível de segurança do intervalo de espera do pop-up do Express Boot [seg.])	Alterar, visualizar ou ocultar.
LAN/WLAN Switching Security Level (Nível de segurança da comutação LAN/WLAN)	Alterar, visualizar ou ocultar.
Embedded Bluetooth Device Radio Security Level (Nível de segurança do rádio de dispositivo Bluetooth integrado)	Alterar, visualizar ou ocultar.
Embedded WWAN Device Radio Security Level (Nível de segurança do rádio de dispositivo WWAN integrado)	Alterar, visualizar ou ocultar.
Power-On Authentication Support Security Level (Nível de segurança do suporte a autenticação na inicialização)	Alterar, visualizar ou ocultar.
Automatic Drivelock Support Security Level (Nível de segurança do suporte a Drivelock automático)	Alterar, visualizar ou ocultar.
Data Execution Prevention Security Level (Nível de segurança da prevenção da execução de dados)	Alterar, visualizar ou ocultar.
SATA Device Mode Security Level (Nível de segurança do modo de dispositivo SATA)	Alterar, visualizar ou ocultar.
USB Ports Security Level (Nível de segurança das portas USB)	Alterar, visualizar ou ocultar.
1394 Port Security Level (Nível de segurança da porta 1394)	Alterar, visualizar ou ocultar.
Express Card Slot Security Level (Nível de segurança do slot para Express Card)	Alterar, visualizar ou ocultar.
Dual Core CPU Security Level (Nível de segurança da CPU Dual Core)	Alterar, visualizar ou ocultar.
Wake on LAN Security Level (Nível de segurança do Wake on LAN)	Alterar, visualizar ou ocultar.
Ambient Light Sensor Security Level (Nível de segurança do sensor de luz ambiente)	Alterar, visualizar ou ocultar.
Secondary Battery Fast Charge Security Level (Nível de segurança do carregamento rápido da bateria secundária)	Alterar, visualizar ou ocultar.
Embedded Security Device Availability Security Level (Nível de segurança da disponibilidade de dispositivos do Embedded Security)	Alterar, visualizar ou ocultar.
HDD Translation Mode Security Level (Nível de segurança do modo de tradução do HD)	Alterar, visualizar ou ocultar.
Fingerprint Device Security Level (Nível de segurança do dispositivo de impressão digital)	Alterar, visualizar ou ocultar.
Optical Disk Drive Security Level (Nível de segurança da unidade de disco óptico)	Alterar, visualizar ou ocultar.

Network Interface Controller (LAN) Security Level (Nível de segurança do controlador de interface de rede [LAN])	Alterar, visualizar ou ocultar.
OS Management of TPM Security Level (Nível de segurança do gerenciamento do TPM pelo SO)	Alterar, visualizar ou ocultar.
Reset of TPM from OS Security Level (Nível de segurança da reinicialização do TPM a partir do SO)	Alterar, visualizar ou ocultar.
Virtualization Technology Security Level (Nível de segurança da tecnologia de virtualização)	Alterar, visualizar ou ocultar.
Terminal Emulation Mode Security Level (Nível de segurança do modo de emulação de terminal)	Alterar, visualizar ou ocultar.
Firmware Verbosity Security Level (Nível de segurança da verbosidade do firmware)	Alterar, visualizar ou ocultar.
Firmware Progress Event Support Security Level (Nível de segurança do suporte a evento de progressão do firmware)	Alterar, visualizar ou ocultar.
Unconfigure AMT Security Level (Desconfigurar nível de segurança AMT)	Alterar, visualizar ou ocultar.
Asset Tracking Number Security Level (Nível de segurança do número de controle de ativo)	Alterar, visualizar ou ocultar.
Ownership Tag Security Level (Nível de segurança da etiqueta de propriedade)	Alterar, visualizar ou ocultar.
Boot Order Security Level (Nível de segurança da seqüência de inicialização)	Alterar, visualizar ou ocultar.
Custom Logo Policy (Política de logotipo personalizado)	Alterar, visualizar ou ocultar.
Unconfigure AMT on next boot Security Level (Nível de segurança de desconfigurar AMT na próxima inicialização)	Alterar, visualizar ou ocultar.
SD Card Boot Security Level (Nível de segurança da inicialização por cartão SD)	Alterar, visualizar ou ocultar.
Boot From EFI File Security Level (Nível de segurança da inicialização pelo arquivo EFI)	Alterar, visualizar ou ocultar.
HP QuickLook 2 Security Level (Nível de segurança do HP QuickLook 2)	Alterar, visualizar ou ocultar.
Wireless Button State Security Level (Nível de segurança do estado do botão de conexão sem fio)	Alterar, visualizar ou ocultar.
Modem Device Security Level (Nível de segurança do dispositivo de modem)	Alterar, visualizar ou ocultar.
Finger Print reset Security Level (Nível de segurança da restauração da impressão digital)	Alterar, visualizar ou ocultar.
HP SpareKey Security Level (Nível de segurança do HP SpareKey)	Alterar, visualizar ou ocultar.
TXT Technology Security Level (Nível de segurança da tecnologia TXT)	Alterar, visualizar ou ocultar.
Diagnostic URL Security Level (Nível de segurança do URL de diagnóstico)	Alterar, visualizar ou ocultar.

7 Embedded Security for HP ProtectTools (somente em determinados modelos)

NOTA: O chip de segurança integrada do módulo de plataforma confiável (TPM) deve estar instalado no computador para que se possa utilizar o Embedded Security for ProtectTools.

Embedded Security for ProtectTools protege contra o acesso não-autorizado a dados ou credenciais do usuário. Este módulo de software fornece os seguintes recursos de segurança:

- Criptografia de pastas e arquivos Enhanced Microsoft® Encryption File System (EFS - Sistema de criptografia de arquivos aprimorado da Microsoft)
- Criação de uma unidade pessoal protegida (PSD) para proteção de dados do usuário
- Funções de gerenciamento de dados, como backup e restauração da hierarquia principal
- Suporte a aplicativos de terceiros (como Microsoft Outlook e Internet Explorer) para operações de certificado digital protegidas durante a utilização do software Embedded Security

O chip TPM de segurança integrada aprimora e ativa outros recursos de segurança do HP ProtectTools Security Manager. Por exemplo, o Credential Manager for HP ProtectTools pode usar o chip integrado como um fator de autenticação quando o usuário faz login no Windows. Em determinados modelos, o chip TPM de segurança integrada também ativa recursos de segurança aprimorados do BIOS acessados através de BIOS Configuration for HP ProtectTools.

Procedimentos de configuração

△ **CUIDADO:** Para reduzir o risco de segurança, é altamente recomendado que o administrador de TI inicialize imediatamente o chip embedded security. Não inicializar o chip embedded security pode possibilitar que um usuário não-autorizado, um invasor de computador ou um vírus tome conta do computador e obtenha controle sobre as tarefas do proprietário, como o manuseio do arquivo de recuperação de emergência e a definição de configurações de acesso do usuário.

Siga as etapas nas duas seções a seguir para ativar e inicializar o chip embedded security.

Ativação do chip embedded security

O chip embedded security deve ser ativado no utilitário de configuração do computador. Esse procedimento não pode ser realizado em BIOS Configuration for HP ProtectTools.

Para ativar o chip embedded security:

1. Abra o Utilitário de configuração ligando ou reiniciando o computador e, em seguida, pressione f10 enquanto a mensagem “f10 = ROM Based Setup” estiver sendo exibida no canto inferior esquerdo da tela.
2. Se uma senha de administrador não tiver sido definida, use as teclas de seta para selecionar **Security** (Segurança), selecione **Setup password** (Senha de configuração) e, em seguida, pressione enter.
3. Digite a senha nas caixas **Nova senha** e **Verificar nova senha** e, em seguida, pressione f10.
4. No menu **Segurança**, use as teclas de chave para selecionar **TPM Segurança Interna** e, em seguida, pressione enter.
5. Em **Segurança Interna**, se o dispositivo estiver oculto, selecione **Disponível**.
6. Selecione **Estado do dispositivo de segurança interna** e altere para **Ativar**.
7. Pressione f10 para aceitar as alterações na configuração de Embedded Security.
8. Para salvar suas preferências e sair do utilitário de configuração do computador, use as teclas de seta para selecionar **File** (Arquivo) e clique em **Save Changes and Exit** (Salvar alterações e sair). Siga as instruções na tela.

Inicialização do chip embedded security

No processo de inicialização do Embedded Security, você irá executar as seguintes tarefas:

- Definir uma senha de proprietário para o chip embedded security que protege o acesso a todas as funções do proprietário do chip embedded security.
- Configurar o arquivo de recuperação de emergência, que é uma área de armazenamento protegida que permite nova criptografia das chaves de usuário básico para todos os usuários.

Para inicializar o chip embedded security:

1. Clique com o botão direito do mouse no ícone HP ProtectTools Security Manager na área de notificação, na extremidade direita da barra de tarefas e, em seguida, selecione **Inicialização de Embedded Security**.

   O assistente de inicialização do ProtectTools Embedded Security é aberto.

2. Siga as instruções na tela.

Configuração da conta de usuário básico

A configuração de uma conta de usuário básico no Embedded Security executa as seguintes tarefas:

- Produz uma chave de usuário básico que protege as informações criptografadas, e define uma senha de chave de usuário básico para proteger a chave de usuário básico.
- Configura uma unidade pessoal protegida (PSD) para armazenamento de pastas e arquivos criptografados.

CUIDADO: Proteja a senha de chave de usuário básico. As informações criptografadas não podem ser acessadas nem recuperadas sem essa senha.

Para configurar uma conta de usuário básico e ativar os recursos de segurança do usuário:

1. Se o Embedded Security User Initialization Wizard (Assistente de Inicialização do Usuário do Embedded Security) não estiver aberto, clique em **Iniciar** , **Todos os Programas** e, em seguida, clique em **HP ProtectTools Security Manager**.
2. No painel esquerdo, clique em **Embedded Security** e, em seguida, clique em **Configurações de usuários**.
3. No painel direito, em **Funções da Embedded Security**, clique em **Configurar**.

   O assistente de inicialização do usuário do Embedded Security é aberto.
4. Siga as instruções na tela.

   NOTA: Para usar e-mail protegido, é preciso primeiro configurar o cliente de e-mail para usar um certificado digital criado com o Embedded Security. Se não houver um certificado digital disponível, é preciso obter um de uma autoridade de certificação. Para obter instruções sobre a configuração de seu e-mail e a obtenção de um certificado digital, consulte a Ajuda do software cliente de e-mail.

Tarefas básicas

Após a configuração da conta de usuário básico, é possível executar as seguintes tarefas:

- Criptografar arquivos e pastas
- Enviar e receber e-mail criptografado

Utilização de Personal Secure Drive (PSD)

Após configurar a PSD, você será solicitado a digitar a senha da chave de usuário básico no próximo login. Se a senha de chave de usuário básico for inserida corretamente, é possível acessar a PSD diretamente do Windows Explorer.

Criptografar arquivos e pastas

Quando trabalhar com arquivos criptografados, observe as seguintes regras:

- Somente arquivos e pastas em partições NTFS podem ser criptografados. Arquivos e pastas em partições FAT não podem ser criptografados.
- Arquivos de sistema e arquivos compactados não podem ser criptografados, e arquivos criptografados não podem ser compactados.
- Pastas temporárias devem ser criptografadas, porque interessam particularmente aos hackers.
- Uma política de recuperação é automaticamente configurada quando um arquivo ou pasta é criptografado pela primeira vez. Essa política garante que se os certificados de criptografia e as chaves de privacidade forem perdidos, será possível usar um agente de recuperação para descriptografar as informações.

Para criptografar arquivos e pastas:

1. Clique com o botão direito no arquivo ou pasta que deseja criptografar.
2. Clique em **Criptografar**.
3. Clique em uma das seguintes opções:
   - **Aplicar alterações a esta pasta somente.**
   - **Aplicar alterações a esta pasta, subpastas e arquivos.**
4. Clique em **OK**.

Enviar e receber e-mail criptografado

O Embedded Security permite o envio e o recebimento de e-mail criptografado, mas os procedimentos variam de acordo com o programa utilizado para acessar e-mail. Para obter mais informações, consulte a Ajuda de software do Embedded Security e a Ajuda de software do seu programa de e-mail.

Alteração da senha de chave de usuário básico

Para alterar a senha de chave de usuário básico:

1. Clique em **Iniciar**, **Todos os Programas** e **HP ProtectTools Security Manager**.
2. No painel esquerdo, clique em **Embedded Security** e, em seguida, clique em **Configurações de usuários**.
3. No painel direito, em **Senha de usuário básico**, clique em **Alterar**.
4. Digite a senha antiga e, em seguida, defina e confirme a nova senha.
5. Clique em **OK**.

Tarefas avançadas

Backup e restauração

O recurso de backup de Embedded Security cria um arquivo que contém informações de certificação a serem restauradas em caso de emergência.

Criação de um arquivo de backup

Para criar um arquivo de backup:

1. Clique em **Iniciar**, **Todos os Programas** e **HP ProtectTools Security Manager**.
2. No painel esquerdo, clique em **Embedded Security** e, em seguida, clique em **Backup**.
3. No painel direito, clique em **Backup**. O assistente de backup do HP Embedded Security for ProtectTools é aberto.
4. Siga as instruções na tela.

Restauração dos dados de certificação do arquivo de backup

Para restaurar dados do arquivo de backup:

1. Clique em **Iniciar**, **Todos os Programas** e **HP ProtectTools Security Manager**.
2. No painel esquerdo, clique em **Embedded Security** e, em seguida, clique em **Backup**.
3. No painel direito, clique em **Restaurar**. O assistente de backup do HP Embedded Security for ProtectTools é aberto.
4. Siga as instruções na tela.

Alteração da senha de proprietário

Para alterar a senha de proprietário:

1. Clique em **Iniciar**, **Todos os Programas** e **HP ProtectTools Security Manager**.
2. No painel esquerdo, clique em **Embedded Security** e, em seguida, clique em **Avançado**.
3. No painel direito, em **Senha de proprietário**, clique em **Alterar**.
4. Digite a senha de proprietário antiga e, em seguida, defina e confirme a nova senha de proprietário.
5. Clique em **OK**.

Redefinição da senha de usuário

Um administrador pode ajudar o usuário a redefinir uma senha esquecida. Para obter mais informações, consulte a Ajuda do software.

Ativação e desativação de Embedded Security

É possível desativar os recursos de Embedded Security se desejar trabalhar sem a função de segurança.

Os recursos de Embedded Security podem ser ativados ou desativados em dois níveis diferentes:

- Desabilitação temporária—Com esta opção, embedded security é automaticamente reativada no reinício do Windows. Essa opção está disponível por padrão para todos os usuários.
- Desabilitação permanente—Com esta opção, a senha de proprietário é requerida para o reinício de Embedded Security. Essa opção está disponível somente para administradores.

Desativação permanente do Embedded Security

Para desativar permanentemente o Embedded Security:

1. Clique em **Iniciar**, **Todos os Programas** e **HP ProtectTools Security Manager**.
2. No painel esquerdo, clique em **Embedded Security** e, em seguida, clique em **Avançado**.
3. No painel direito, em **Embedded Security**, clique em **Desativar**.
4. Insira sua senha de proprietário no prompt e, em seguida, clique em **OK**.

Ativação do Embedded Security após desativação permanente

Para ativar Embedded Security após desativá-lo permanentemente:

1. Clique em **Iniciar**, **Todos os Programas** e **HP ProtectTools Security Manager**.
2. No painel esquerdo, clique em **Embedded Security** e, em seguida, clique em **Avançado**.
3. No painel direito, em **Embedded Security**, clique em **Ativar**.
4. Insira sua senha de proprietário no prompt e, em seguida, clique em **OK**.

Migração de chaves com o assistente de migração

A migração é uma tarefa avançada de administrador que permite o gerenciamento, a restauração e a transferência de chaves e certificados.

Para obter detalhes sobre a migração, consulte a Ajuda de software do Embedded Security.

8 Device Access Manager for HP ProtectTools (somente em determinados modelos)

Essa ferramenta de segurança está disponível somente para administradores. O Device Access Manager for HP ProtectTools (Gerenciador de Acesso a Dispositivos para HP ProtectTools) possui os seguintes recursos de segurança que fornecem proteção contra acesso não-autorizado a dispositivos anexados a seu sistema de computador:

- Perfis de dispositivos que são criados para cada usuário para definir o acesso a dispositivos
- Acesso a dispositivos que pode ser concedido ou negado com base em associações de grupos

Inicializar serviços de segundo plano

Para perfis de dispositivo a serem aplicados, o serviço de segundo plano de bloqueio/auditoria de dispositivo HP ProtectTools deve ser executado. Quando tentar aplicar perfis de dispositivo pela primeira vez, o HP ProtectTools Security Manager abre uma caixa de diálogo para perguntar se deseja iniciar o serviço de segundo plano. Clique em **Sim** para iniciar o serviço de segundo plano e defini-lo para iniciar automaticamente sempre que o sistema inicializar.

Configuração simples

Este recurso permite que proíba o acesso às seguintes classes de dispositivos:

- Dispositivos USB para todos que não sejam administradores
- Toda mídia removível (disquete, pen drives, etc.) para todos que não sejam administradores
- Todas as unidades de DVD/CD-ROM para todos que não sejam administradores
- Todas as portas seriais e paralelas para todos que não sejam administradores

Para negar o acesso a uma classe de dispositivo para todos que não sejam administradores:

1. Clique em **Iniciar**, **Todos os Programas** e **HP ProtectTools Security Manager**.
2. No painel esquerdo, clique em **Gerenciador de Acesso a Dispositivos**, em seguida, clique em **Configuração simples**.
3. No painel direito, marque a caixa de seleção de um dispositivo para negar acesso.
4. Clique em **Aplicar**.

   NOTA: Se serviço de segundo plano não tiver executando, ele será solicitado a iniciar agora. Clique em **Sim** para permiti-lo.

5. Clique em **OK**.

Configuração de classe de dispositivo (avançado)

Estão disponíveis mais seleções para permitir que usuários específicos ou grupos de usuários tenham acesso autorizado ou proibido a tipos de dispositivo.

Adição de um usuário ou grupo

1. Clique em **Iniciar**, **Todos os Programas** e **HP ProtectTools Security Manager**.
2. No painel esquerdo, clique em **Gerenciador de Acesso a Dispositivos**, em seguida, clique em **Configuração de classe de dispositivo**.
3. Na lista de dispositivo, clique na classe de dispositivo que deseja configurar.
4. Clique em **Adicionar**. A caixa de diálogo de **Selecione usuários ou grupos** é aberta.
5. Clique em **Advanced** (Avançado) e, em seguida, clique em **Find Now** (Localizar agora) para pesquisar usuários ou grupos para adicionar.
6. Clique no usuário ou grupo a ser adicionado à lista de usuários e grupos disponíveis e, em seguida, clique em **OK**.
7. Clique em **OK**.

Remoção de um usuário ou grupo

1. Clique em **Iniciar**, **Todos os Programas** e **HP ProtectTools Security Manager**.
2. No painel esquerdo, clique em **Gerenciador de Acesso a Dispositivos**, em seguida, clique em **Configuração de classe de dispositivo**.
3. Na lista de dispositivo, clique na classe de dispositivo que deseja configurar.
4. Clique no usuário ou grupo que deseja remover e, em seguida clique em **Remover**.
5. Clique em **Aplicar** em seguida, clique em **OK**.

Negar acesso para usuário ou grupo

1. Clique em **Iniciar**, **Todos os Programas** e **HP ProtectTools Security Manager**.
2. No painel esquerdo, clique em **Gerenciador de Acesso a Dispositivos**, em seguida, clique em **Configuração de classe de dispositivo**.
3. Na lista de dispositivo, clique na classe de dispositivo que deseja configurar.
4. Em **Usuários/Grupos**, clique no usuário ou grupo ao qual negar o acesso.
5. Clique em **Negar**, próximo ao usuário ou grupo aos quais será impedido acesso.
6. Clique em **Aplicar** e, em seguida, clique em **OK**.

Permitir acesso a uma classe de dispositivo para um usuário ou grupo

Você pode permitir o acesso de um usuário a uma classe de dispositivo a qual foi impedido o acesso para todos os outros membros do grupo de usuários.

Para permitir acesso a um usuário mas não ao grupo:

1. Clique em **Iniciar**, **Todos os Programas** e **HP ProtectTools Security Manager**.
2. No painel esquerdo, clique em **Gerenciador de Acesso a Dispositivos**, em seguida, clique em **Configuração de classe de dispositivo**.
3. Clique na classe de dispositivo que deseja configurar na lista de dispositivo.
4. Em **Usuários/Grupos**, adicionar o grupo ao qual será impedido acesso.
5. Clique em **Negar**, próximo ao grupo ao qual será impedido acesso.
6. Navegue até a pasta abaixo que contém a caixa requerida e adicione um usuário específico. Clique em **Permitir** para permitir o acesso desse usuário.
7. Clique em **Aplicar** e, em seguida, clique em **OK**.

Permitir acesso a um dispositivo específico para um usuário do grupo

Você pode permitir o acesso de um usuário a um dispositivo específico ao qual foi impedido acesso para todos os outros membros do grupo de usuários para todos os dispositivos da classe.

Para permitir acesso de um usuário a um dispositivo específico mas não ao grupo:

1. Clique em **Iniciar**, **Todos os Programas** e **HP ProtectTools Security Manager**.
2. No painel esquerdo, clique em **Gerenciador de Acesso a Dispositivos**, em seguida, clique em **Configuração de classe de dispositivo**.
3. Na lista de dispositivo, clique na classe de dispositivo que deseja configurar, em seguida navegue na pasta abaixo.
4. Em **Usuários/Grupos**, adicionar o grupo ao qual será impedido acesso.
5. Clique em **Impedir**, próximo ao grupo ao qual será impedido acesso.
6. Navegue até o dispositivo específico que será permitido ao usuário, na lista de dispositivo.
7. Clique em **Adicionar**. A caixa de diálogo de **Selecionar usuários ou grupos** é aberta.
8. Clique em **Advanced** (Avançado) e, em seguida, clique em **Find Now** (Localizar agora) para pesquisar usuários ou grupos para adicionar.
9. Clique em um usuário para permitir acesso, em seguida clique em **OK**.
10. Clique em **Permitir** para permitir o acesso desse usuário.
11. Clique em **Aplicar** e, em seguida, clique em **OK**.

9 Solução de problemas

Credential Manager for HP ProtectTools

Descrição resumida	Detalhes	Solução
Utilizando a opção Credential Manager Network Accounts (Contas de rede do Credential Manager), um usuário pode selecionar a conta de domínio na qual efetuar o login. Quando a autenticação por TPM é utilizada, essa opção não fica disponível. Todos os outros métodos de autenticação funcionam corretamente.	Utilizando a autenticação por TPM, o usuário efetua o login somente no computador local.	Utilizando as ferramentas de Single Sign On do Credential Manager, o usuário pode autenticar outras contas.
Smart cards e tokens USB não estarão disponíveis no Credential Manager se tiverem sido instalados após a instalação do Credential Manager.	Para usar smart cards ou tokens USB no Credential Manager, o software de suporte (drivers, fornecedores de PKCS#11, etc.) deve ser instalado antes da instalação do Credential Manager. Se o Credential Manager já estiver instalado, execute as seguintes etapas após a instalação do software de suporte de smart card ou token:	Efetue login no Credential Manager. No HP ProtectTools Security Manager, clique em **Credential Manager**, **Advanced Settings** (Configurações avançadas) e, em seguida, clique na guia **Smart Cards and Tokens** (Smart cards e tokens). Uma lista dos tokens disponíveis é exibida em Local Tokens (Tokens locais). Acesse um menu instantâneo clicando com o botão direito no nó de Local Tokens (Tokens locais) e selecione Scan for New Smart Cards and Tokens (Procurar novos smart cards e tokens). Reinicie o computador, se solicitado.
Algumas páginas web de aplicativos geram erros que evitam que o usuário execute ou conclua tarefas.	Alguns aplicativos web param de funcionar e relatam erros devido ao padrão de funcionalidade de desativação do Single Sign On. Por exemplo, um **!** em um triângulo amarelo é exibida no Internet Explorer, indicando a ocorrência de um erro.	O Single Sign On do Credential Manager não suporta todas as interfaces Web de software. Desative o suporte ao Single Sign On para a página da Web específica desligando o suporte ao Single Sign On. Consulte a documentação completa sobre o Single Sign On, disponível nos arquivos de Ajuda do software do Credential Manager. Se um Single Sign On específico não puder ser desativado para um determinado aplicativo, entre em contato com o suporte técnico da HP e solicite suporte de nível 3 através do seu contato na HP Service.
A opção **Browse for Virtual Token** (Procurar token virtual) não é	O usuário não pode mover o local de um token virtual registrado no Credential Manager, pois a opção para procura foi	A opção de procura foi removida porque permitia a não-usuários excluir e renomear arquivos e controlar o Windows.

Descrição resumida	Detalhes	Solução
exibida durante o processo de login.	removida visando reduzir os riscos de segurança.	
Os administradores de domínio não podem alterar a senha do Windows, mesmo com autorização.	Isso ocorre depois que um administrador de domínio acessa um domínio e registra a identidade do domínio com o Credential Manager, utilizando uma conta com privilégios de administrador no domínio e no computador local. Quando o administrador de domínio tenta alterar a senha do Windows a partir do Credential Manager, ele obtém uma falha de erro de login: **Restrição de conta de usuário**.	O Credential Manager não pode alterar a senha de uma conta de usuário em um domínio através da opção **Change Windows password** (Alterar senha do Windows). O Credential Manager pode alterar somente senhas de contas no computador local. O usuário de um domínio pode alterar sua senha através da opção **Change password** (Alterar senha) de **Windows security** (Segurança do Windows), mas, uma vez que o usuário de um domínio não possui uma conta física no computador local, o Credential Manager só pode alterar a senha utilizada para login.
O Credential Manager tem problemas de incompatibilidade com a biblioteca GINA de senhas do Corel WordPerfect 12.	Se o usuário efetua login no Credential Manager, cria um documento no WordPerfect e salva com proteção por senha, o Credential Manager não pode detectar ou reconhecer, seja de forma manual ou automática, a biblioteca GINA de senhas.	A HP está pesquisando uma solução alternativa para aprimoramentos futuros do produto.
O Credential Manager não reconhece o botão **Conectar** na tela.	Se as credenciais do Single Sign On para o Remote Desktop Connection (RDP) forem definidas para **Conectar**, quando o Single Sign On reiniciado, ele sempre irá inserir **Salvar como** em vez de **Conectar**.	A HP está pesquisando uma solução alternativa para aprimoramentos futuros do produto.
Os usuários podem perder todas as credenciais do Credential Manager protegidas pelo módulo TPM.	Se o módulo TPM for removido ou danificado, os usuários perderão todas as credenciais protegidas pelo TPM.	Isso foi projetado desta maneira. O módulo TPM é projetado para proteger as credenciais do Credential Manager. A HP recomenda que o usuário faça o backup de sua identidade no Credential Manager antes de remover o módulo TPM.
O usuário não é capaz de efetuar login no Credential Manager após passar do modo de suspensão para a hibernação somente no Windows XP Service Pack 1.	Apos permitir que o sistema passe para a hibernação e o modo de suspensão, o administrador ou o usuário não consegue fazer login no Credential Manager e a tela de login do Windows permanece exibida, independentemente da credencial de login (senha, impressão digital ou Java Card) que se encontra selecionada.	Atualize o Windows com o Service Pack 2 usando o Windows Update. Consulte o artigo 813301 da base de conhecimento da Microsoft em http://www.microsoft.com para obter mais informações sobre a causa do problema. Para efetuar o login, o usuário deve selecionar o Credential Manager e efetuar o login. Após efetuar o login no Credential Manager, o usuário é solicitado a efetuar o login no Windows (o usuário pode ter que selecionar a opção de login do Windows) para concluir o processo de login. Se o usuário efetuar o login no Windows primeiro, então ele deve efetuar o login no Credential Manager manualmente.
A restauração do Embedded Security causa uma falha no Credential Manager.	O CM não registra credenciais depois que a ROM é restaurada com as configurações de fábrica.	O Credential Manager falha ao acessar o módulo TPM se a ROM for restaurada com as configurações de fábrica após a instalação do Credential Manager. O chip de segurança integrada TPM pode ser ativado usando o utilitário de configuração do computador f10, o BIOS Configuration ou o HP Client Manager. Para ativar o chip de segurança integrada TPM utilizando o utilitário de configuração do computador, siga estas etapas:

Descrição resumida	Detalhes	Solução
		1. Abra o utilitário de configuração do computador ligando ou reiniciando o computador e, em seguida, pressione f10 enquanto a mensagem **f10 = ROM Based Setup** estiver sendo exibida no canto inferior esquerdo da tela. **2.** Use as teclas de seta para clicar em **Security** (Segurança) e depois em**Setup Password** (Senha de configuração). Defina uma senha. **3.** Selecione **Dispositivo de embedded security**. **4.** Utilize as teclas de seta para selecionar **Dispositivo de embedded security – Desativar**. Utilize as teclas de seta para alterar para **Dispositivo de embedded security – Ativar**. **5.** Clique em **Enable** (Ativar) e, em seguida, clique em **Save changes and exit** (Salvar alterações e sair). A HP está investigando opções de solução para futuros lançamentos de software ao cliente.
O processo de segurança **Restore Identity** (Restaurar identidade) perde a associação com o token virtual.	Quando o usuário restaurar a identidade, o Credential Manager pode perder a associação com o local do token virtual na tela de login. Embora o Credential Manager tenha o token virtual registrado, o usuário deve registrar novamente o token para restaurar a associação.	Esta é uma decisão de projeto. Ao desinstalar o Credential Manager sem manter as identidades, a parte sistema (servidor) do token é destruída, de modo que o token não pode mais ser utilizado para efetuar o login, mesmo se a parte cliente do token for restaurada por meio da restauração de identidade. A HP está investigando opções de longo prazo para uma solução.

Embedded Security for HP ProtectTools (somente em determinados modelos)

Descrição resumida	Detalhes	Solução
Criptografia de pastas, subpastas e arquivos na unidade PSD provocam uma mensagem de erro.	Se o usuário copiar arquivos e pastas para a unidade PSD e tentar criptografar pastas/arquivos ou pastas/subpastas, a mensagem **Error Applying Attributes** (Erro na aplicação de atributos) é exibida. O usuário pode criptografar os mesmos arquivos na unidade C:\ ou em uma unidade de disco rígido adicional instalada.	Isso foi projetado desta maneira. A ação de mover arquivos/pastas para a unidade PSD faz com que estes sejam automaticamente criptografados. Não há necessidade de "criptografar novamente" os arquivos/pastas. Tentar criptografá-los novamente na unidade PSD utilizando EFS produz esta mensagem de erro.
Não é possível assumir a propriedade com outro sistema operacional na plataforma MultiBoot.	Se uma unidade estiver configurada para inicialização de múltiplos sistemas operacionais, a propriedade só pode ser definida com o assistente de inicialização de plataforma em um sistema operacional.	Esta é uma decisão de projeto por questões de segurança.
Um administrador não-autorizado pode visualizar, excluir, renomear ou mover o conteúdo de pastas EFS criptografadas.	A criptografia de uma pasta não impede um usuário não autorizado com privilégios administrativos de visualizar, excluir, renomear ou mover o conteúdo da pasta.	Isso foi projetado desta maneira. Este é um recurso do EFS não do Embedded Security TPM. O Embedded Security utiliza o software EFS da Microsoft e preserva os direitos de acesso a pastas/arquivos para todos os administradores.
Não há opções de criptografia para o usuário ao tentar restaurar a unidade de disco rígido utilizando o FAT32.	Se o usuário tentar restaurar a unidade de disco rígido utilizando o FAT32, não haverá opções de criptografia para qualquer arquivo/pasta utilizando o EFS.	Isso foi projetado desta maneira. O software não deve ser instalado em uma restauração com uma partição FAT32. O Microsoft EFS é suportado somente no NTFS e não funciona no FAT32. Este é um recurso do Microsoft EFS e não está relacionado ao software HP ProtectTools.
O usuário é capaz de criptografar ou excluir o arquivo XML do arquivo de recuperação.	Por projeto, as ACLs (listas de controle de acesso) para esta pasta não são definidas; portanto, um usuário pode inadvertidamente ou intencionalmente criptografar ou excluir o arquivo, tornando-o inacessível. Após esse arquivo ter sido criptografado ou excluído, ninguém pode usar o software do módulo TPM.	Esta foi uma decisão de projeto. Os usuários possuem direitos de acesso a um arquivo de emergência de modo que podem salvar/atualizar sua cópia de backup da Chave de usuário básico. Os usuários devem ser instruídos a nunca criptografar ou excluir os arquivos do arquivo de recuperação.
A interação do Embedded Security EFS com o Symantec Antivirus ou o McAfee Total Protection gera períodos de criptografia/ descriptografia e verificação mais longos.	Arquivos criptografados interferem na verificação de vírus do Symantec Antivirus ou do McAfee Total Protection. A criptografia de arquivos utilizando o Embedded Security EFS demora mais quando o Symantec Antivirus ou o McAfee Total Protection está em execução.	Para diminuir o tempo necessário para verificação de arquivos do Embedded Security EFS, o usuário pode digitar a senha de criptografia ou descriptografar antes de começar a verificação. Para diminuir o tempo necessário para criptografar/ descriptografar dados utilizando o Embedded Security EFS, o usuário deve desativar a proteção automática do Symantec Antivirus ou McAfee Total Protection.
O arquivo de recuperação de emergência não pode ser salvo em mídia removível.	Se o usuário inserir um cartão de memória MultiMediaCard ou Secure Digital (SD) ao criar o caminho do arquivo de recuperação de emergência durante a inicialização do Embedded	Esta foi uma decisão de projeto. O armazenamento do arquivo de recuperação em mídia removível não é suportado. O arquivo de recuperação pode ser armazenado em uma unidade

Descrição resumida	Detalhes	Solução
	Security, uma mensagem de erro é exibida.	de rede ou em uma outra unidade local diferente da unidade C.
Ocorrem erros após uma queda de energia interromper a inicialização do Embedded Security.	Se houver uma queda de energia durante a inicialização do chip Embedded Security, os seguintes problemas ocorrem: • Ao tentar iniciar o assistente de inicialização do Embedded Security, a seguinte mensagem de erro é exibida: **The Embedded security cannot be initialized since the Embedded Security chip already has an Embedded Security owner** (O recurso Embedded Security não pode ser inicializado, pois o chip do Embedded Security já possui um proprietário do tipo Embedded Security). • Ao tentar iniciar o assistente de inicialização do usuário, a seguinte mensagem de erro é exibida: **The Embedded security is not initialized. To use the wizard, the Embedded Security must be initialized first** (O Embedded Security não foi inicializado. Para usar o assistente, o Embedded Security deve ser inicializado primeiro).	Execute o procedimento a seguir para recuperar depois de uma queda de energia: **NOTA:** Use as teclas de seta para selecionar diversos menus, itens de menu e alterar valores (a menos que especificado de forma diferente). 1. Ligue ou reinicie o computador. 2. Pressione f10 quando a mensagem **f10=Setup** for exibida na tela. 3. Selecione a opção de idioma apropriada. 4. Pressione enter. 5. Selecione **Security** (Segurança) e, em seguida, clique em **Embedded Security**. 6. Defina a opção **Dispositivo Embedded Security** como **Ativar**. 7. Pressione f10 para aceitar a alteração. 8. Selecione **File** (Arquivo) e, em seguida, clique em **Save changes and exit** (Salvar alterações e sair). 9. Pressione enter. 10. Pressione f10 para salvar as alterações e sair do utilitário.
A senha do utilitário de configuração do computador (**f10**) pode ser removida após a ativação do módulo TPM.	Ativar o módulo TPM requer uma senha do utilitário de configuração do computador (**f10**). Quando o módulo tiver sido ativado, o usuário pode remover a senha. Isso permite que qualquer pessoa com acesso direto ao sistema reinicialize o módulo TPM e cause uma possível perda de dados.	Esta foi uma decisão de projeto. A senha do utilitário de configuração do computador (**f10**) somente pode ser removida pelo usuário que a conhece. Entretanto, a HP recomenda fortemente manter a senha do utilitário de configuração do computador (**f10**) sempre protegida.
A caixa de senha do PSD não é mais exibida quando o sistema se torna ativo após um período em espera	Quando um usuário faz login no sistema após a criação de uma unidade PSD, o módulo TPM solicita a senha de usuário básico. Se o usuário não digitar a senha e o sistema iniciar o modo de espera, a caixa de diálogo de senha não fica mais disponível quando o usuário retoma.	Esta é uma decisão de projeto. O usuário precisa efetuar o logoff e um novo login para visualizar novamente a caixa de senha PSD.
Nenhuma senha é requerida para alterar as políticas da plataforma de segurança.	O acesso às políticas da plataforma de segurança (tanto máquina como usuário) não exige uma senha TPM para usuários com privilégios administrativos no sistema.	Esta é uma decisão de projeto. Qualquer administrador pode modificar as políticas da plataforma de segurança com ou sem a inicialização de usuário TPM.
Quando um certificado é visualizado, ele é exibido como não-confiável.	Após a configuração do HP ProtectTools e execução do assistente de inicialização do usuário, o usuário pode visualizar o certificado emitido; entretanto, quando o certificado é visualizado, ele é exibido como não-	Os certificados auto-assinados não são confiáveis. Em um ambiente empresarial devidamente configurado, os certificados EFS são emitidos pelas autoridades de certificação on-line e são considerados confiáveis.

Descrição resumida	Detalhes	Solução
	confiável. Embora o certificado possa ser instalado neste momento clicando-se no botão de instalação, instalá-lo não o torna confiável.	
Ocorre um erro intermitente de criptografia e descriptografia: **The process cannot access the file because it is being used by another process** (O processo não pode acessar o arquivo porque ele está sendo utilizado por outro processo).	Esse é um erro extremamente intermitente durante a criptografia ou descriptografia de arquivos e ocorre porque o arquivo está sendo utilizado por outro processo, ainda que o referido arquivo ou pasta não esteja sendo processado pelo sistema operacional ou outros aplicativos.	Para resolver a falha: 1. Reinicie o sistema. 2. Efetue o log off. 3. Efetue novamente o login.
Ocorre perda de dados em um armazenamento removível se a mídia de armazenamento é removida antes da conclusão da geração ou da transferência dos novos dados.	A remoção de uma mídia de armazenamento, como uma unidade de disco rígido MultiBay, não afeta a exibição da unidade PSD como disponível e não gera erros quando se adiciona/modifica dados na unidade PSD. Após o sistema ser reiniciado, a unidade PSD não reflete as alterações de arquivo que ocorreram enquanto o armazenamento removível estava indisponível.	Não remova uma unidade PSD antes da conclusão da geração ou transferência de dados. Esse problema só ocorre se o usuário acessar a unidade PSD e, em seguida, remover a unidade de disco rígido antes da conclusão da geração ou transferência de novos dados. Se o usuário tentar acessar a unidade PSD quando a unidade de disco rígido removível não estiver presente, é exibida uma mensagem de erro informando que **o dispositivo não está pronto**.
Durante a desinstalação, se o usuário não tiver inicializado o Usuário básico e abrir a ferramenta de administração, a opção **Desativar** não estará disponível e o desinstalador não continuará até que a ferramenta de administração seja fechada.	O usuário tem a opção de desinstalar sem desativar o módulo TPM ou desativando primeiro o TPM (através da ferramenta de administração) e, em seguida, realizando a desinstalação. O acesso à ferramenta de administração requer a inicialização da chave de usuário básico. Se a inicialização básica não tive ocorrido, todas as opções estarão inacessíveis para o usuário. Como o usuário escolheu explicitamente abrir a ferramenta de administração (clicando em **Yes** (Sim) na caixa de diálogo **Click Yes to open Embedded Security Administration tool** (Clique em Sim para abrir a ferramenta de administração do Embedded Security), a desinstalação aguarda até que a ferramenta de administração seja fechada. Se o usuário clicar em **No** (Não) na caixa de diálogo, a ferramenta de administração não abre e a desinstalação continua.	A ferramenta de administração é utilizada para desativar o chip TPM, mas essa opção não está disponível a menos que a chave de usuário básico já tenha sido inicializada. Se ela não tiver sido inicializada, selecione **OK** ou **Cancelar** para continuar com a desinstalação.
Ocorre um travamento intermitente do sistema após a criação de uma unidade PSD em contas de 2 usuários e a utilização do recurso de comutação rápida de usuário (fast-user-	Quando se utiliza a comutação rápida com um mínimo de RAM, é possível que o sistema trave com a tela em branco e o teclado e o mouse parem de responder, em vez do sistema exibir a tela de boas-vindas (login).	Suspeita-se que a causa-raiz seja um problema de sincronia nas configurações de pouca memória. A placa gráfica integrada utiliza a arquitetura UMA que consome 8 MB de memória, deixando apenas 120 MB disponíveis para o usuário. O erro é gerado quando estes 120 MB são compartilhados por ambos os

Descrição resumida	Detalhes	Solução
switching) nas configurações de sistema 128 MB.		usuários que efetuaram login e estão usando o recurso de comutação rápida de usuário. A solução provisória é reinicializar o sistema e aumentar a configuração da memória (a HP não fornece configurações de 128 MB com módulos de segurança).
A Autenticação de Usuário EFS (solicitação de senha) expira com **acesso negado**.	O prompt de senha da Autenticação de Usuário EFS reaparece após o usuário clicar em **OK** ou o sistema sair do modo de espera.	Esta é uma decisão de projeto para evitar problemas com o MS EFS, onde um watchdog timer de 30 segundos foi criado para gerar a mensagem de erro.
Pequeno problema de truncamento durante a configuração do idioma japonês é observado em descrições funcionais.	As descrições funcionais durante as opções de configuração personalizada, durante o assistente de instalação, estão truncadas.	A HP corrigirá este problema em uma versão futura.
A criptografia EFS funciona sem que uma senha seja digitada no prompt.	Ao permitir que o prompt de senha do usuário tenha seu tempo esgotado, a criptografia de um arquivo ou pasta continua disponível.	A capacidade de criptografar não requer a autenticação de senha, pois esse é um recurso da criptografia Microsoft EFS. A descriptografia exigirá que a senha do usuário seja fornecida.
O recurso de e-mail protegido é suportado, mesmo quando não é especificado no assistente de inicialização do usuário ou quando sua configuração está desativada nas políticas do usuário.	O software e o assistente do Embedded Security não controlam as configurações de um cliente de e-mail (Outlook, Outlook Express ou Netscape).	Esse comportamento foi projetado desta maneira. A definição de configurações de e-mail do TPM não impede a edição de configurações de criptografia diretamente em um cliente de e-mail. A utilização de e-mail protegido é definida e controlada por aplicativos de terceiros. O assistente da HP permite o link com três aplicativos de referência para personalização imediata.
A execução de implantação em larga escala por uma segunda vez no mesmo PC ou em um PC previamente inicializado sobregrava os arquivos de recuperação de emergência e de token de emergência. Os novos arquivo não servem para recuperação.	A execução de uma implantação em larga escala em qualquer sistema HP ProtectTools Embedded Security previamente inicializado inutiliza arquivos e tokens de recuperação existentes substituindo aqueles arquivos XML.	A HP está trabalhando para resolver o problema de substituição de arquivo XML e fornecerá uma solução em um SoftPaq futuro.
Os scripts de login automatizado não funcionam durante a restauração do usuário no Embedded Security.	O erro ocorre após o usuário executar as seguintes ações: ● Inicializar o proprietário e usuário no Embedded Security (utilizando os locais padrão – **Meus documentos**). ● Restaurar o chip com as configurações de fábrica no BIOS. ● Reiniciar o computador. ● Iniciar a restauração do Embedded Security. Durante o processo de restauração, o Credential Manager pergunta se o sistema pode automatizar o login usando o	Clique no botão **Procurar** na tela para selecionar o local e o processo de restauração continuará.

Descrição resumida	Detalhes	Solução
	Infineon TPM User Authentication (Autenticação de usuário TPM Infineon). Se o usuário selecionar **Sim**, o local do SPEmRecToken é automaticamente exibido na caixa de texto. Mesmo que este local esteja correto, a seguinte mensagem de erro é exibida: **Nenhum token de recuperação de emergência foi fornecido. Selecione o local de onde o token de recuperação de emergência deve ser recuperado.**	
As unidades PSD de vários usuários não funcionam em um ambiente de comutação rápida de usuário.	Esse erro ocorre quando vários usuários foram criados e receberam unidades PSD com a mesma letra. Se for feita uma tentativa de comutação rápida de usuário entre os usuários quando a PSD está carregada, a PSD do segundo usuário não estará disponível.	A PSD do segundo usuário estará disponível somente se for reconfigurada para usar outra letra de unidade ou se o primeiro usuário efetuar o logoff.
A PSD é desativada e não pode ser excluída após a formatação da unidade de disco rígido na qual foi gerada.	O ícone da PSD ainda estará visível, mas a mensagem de erro **unidade inacessível** será exibida quando o usuário tentar acessá-la. O usuário não pode excluir a PSD e a seguinte mensagem de erro é exibida: **your PSD is still in use, please be sure that your PSD contains no open files and is not accessed by another process** (sua PSD ainda está em uso; certifique-se de que sua PSD não contém arquivos abertos e não está sendo acessada por outro processo). O usuário deve reiniciar o sistema para excluir a PSD, que não será carregada após a reinicialização.	Conforme decisão de projeto: Se um cliente força a exclusão ou desconecta do local de armazenamento dos dados PSD, a emulação de unidade PSD do Embedded Security continuará a funcionar e produzirá erros com base na ausência de comunicação com os dados faltantes. Solução: Na reinicialização seguinte, a emulação não consegue carregar e o usuário pode excluir a emulação de PDS anterior e criar um novo PSD.
É detectado um erro interno quando o usuário está restaurando a partir do arquivo de backup automático.	No Embedded Security, se o usuário clicar na opção **Restore under Backup** (Restaurar de backup) para restaurar a partir do arquivo de backup automático e, em seguida, selecionar **SPSystemBackup.xml**, o assistente de restauração falhará e a seguinte mensagem de erro será exibida: **The selected Backup Archive does not match the restore reason. Please select another archive and continue.** (O Arquivo de backup automático selecionado não corresponde ao motivo da restauração. Selecione um outro arquivo e continue.).	Se o usuário selecionar **SpSystemBackup.xml** quando o SpBackupArchive.xml for solicitado, o assistente do Embedded Security falhará e exibirá a seguinte mensagem: **An internal Embedded Security error has been detected** (Foi detectado um erro interno do Embedded Security). O usuário deve selecionar o arquivo XML correto para corresponder ao motivo requerido. Os processos estão operando conforme projetado e funcionam corretamente; entretanto, a mensagem de erro interno do Embedded Security não é clara e deveria conter uma mensagem mais apropriada. A HP está trabalhando para otimizar isso em produtos futuros.
O sistema de segurança exibe um erro de restauração com vários usuários.	Durante o processo de restauração, se o administrador selecionar usuários para restaurar, os usuários não selecionados não poderão restaurar as chaves ao tentar restaurar mais tarde. Uma mensagem de erro **falha no processo de decodificação** é exibida.	Os usuários não-selecionados podem ser restaurados através da reinicialização do TPM, da execução do processo de restauração e da seleção de todos os usuários antes que o próximo backup diário seja executado. Se o backup automático for executado, ele substituirá os usuários não-restaurados e seus dados serão perdidos. Se um novo sistema de backup for

Descrição resumida	Detalhes	Solução
		armazenado, os usuários não-selecionados anteriores não poderão ser restaurados. Além disso, o usuário precisa restaurar o backup do sistema inteiro. Um backup de arquivo pode ser restaurado de forma individual.
A restauração da ROM do sistema para os valores padrão oculta o TPM.	A restauração da ROM do sistema com os valores padrão faz com que o TPM fique oculto para o Windows. Isso impede que o software de segurança opere corretamente e torna os dados criptografados por TPM inacessíveis.	Exibir o TPM no BIOS: Abra o utilitário de configuração do computador (**f10**), navegue até **Security** (Segurança) > **Device security** (Segurança do dispositivo) e, em seguida, modifique o campo de **Hidden** (Oculto) para **Available** (Disponível).
O backup automático não funciona com a unidade mapeada.	Quando um administrador configura o backup automático no Embedded Security, ele cria uma entrada em **Windows** > **Tarefas** > **Tarefas agendadas**. Essa Tarefa agendada do Windows é configurada de forma a usar o NT AUTHORITY\SYSTEM para obter direitos para executar o backup. Isso funciona corretamente para qualquer unidade local. Quando o administrador, em vez de configurar o backup automático para salvar em uma unidade de disco mapeada, o processo falha, pois NT AUTHORITY\SYSTEM não possui os direitos para utilizar a unidade mapeada. Se o backup automático for agendado para ocorrer após o login, o ícone Embedded Security TNA exibe a seguinte mensagem: **The Backup Archive location is currently not accessible. Click here if you want to backup to a temporary archive until the Backup Archive is accessible again.** (A localização do arquivo de backup não está acessível no momento. Clique aqui para fazer o backup em um arquivo temporário até que o arquivo de backup esteja novamente acessível). Se o backup automático for agendado para uma hora específica, entretanto, o backup falhará sem exibir mensagem de erro.	A solução é alterar o NT AUTHORITY\SYSTEM para (nome do computador)\(nome do administrador) Esta é a configuração padrão, se a tarefa agendada for criada manualmente. A HP está trabalhando para oferecer versões futuras do produto com configurações padrão que incluam nome do computador\nome do administrador.
O Embedded Security não pode ser temporariamente desativado na GUI do Embedded Security.	O software 4.0 atual foi criado para implementações HP Notebook 1.1B, bem como para oferecer suporte às implementações HP Desktop 1.2. Esta opção para desativar ainda é oferecida na interface de software das plataformas TPM 1.1.	A HP corrigirá este problema em uma versão futura.

Device Access Manager for HP ProtectTools

Descrição resumida	Detalhes	Solução
Os usuários tiveram o acesso a dispositivos negado no Device Access Manager, mas os dispositivos ainda estão acessíveis.	Os recursos de configuração simples e/ou configuração de classe de dispositivos (Simple Configuration e/ou Device Class Configuration) foram utilizados no Device Access Manager para negar o acesso de usuários a dispositivos. Apesar de terem o acesso negado, os usuários ainda podem acessar os dispositivos.	Verifique se o serviço de bloqueio de dispositivos do HP ProtectTools foi iniciado. Como um usuário administrativo, vá para **Painel de controle > Ferramentas Administrativas > Serviços**. Na janela **Serviços**, procure o serviço **HP ProtectTools Device Locking/Auditing** (Bloqueio/auditoria de dispositivos do HP ProtectTools). Verifique se o serviço foi iniciado e se o tipo de inicialização é **Automatic** (Automática).
Um usuário teve acesso a um dispositivo sem que isso estivesse previsto, ou um usuário teve o acesso negado a um dispositivo quando o acesso estava previsto.	O Device Access Manager foi utilizado para negar o acesso de usuários a alguns dispositivos e permitir o acesso de usuários a outros dispositivos. Quando o usuário está utilizando o sistema, ele pode acessar dispositivos para os quais acredita que o Device Access Manager tenha negado acesso, e ter o acesso negado a dispositivos para os quais acredita que o Device Access Manager devesse permitir o acesso.	O Device Class Configuration no Device Access Manager deve ser utilizado para investigar as configurações de dispositivo dos usuários. Clique em **Security Manager**, **Device Access Manager** e, em seguida, clique em **Device Class Configuration** (Configuração de classe de dispositivo). Expanda os níveis na árvore de classes de dispositivos e reveja as configurações aplicáveis ao usuário. Verifique se há permissões do tipo "Deny" (Negar) definidas para o usuário ou qualquer grupo do Windows ao qual ele possa pertencer, por ex., Usuários, Administradores.
Permitir ou negar – qual dos dois tem precedência?	No Device Class Configuration, a seguinte configuração foi definida: • A permissão Allow (Permitir) foi concedida a um grupo do Windows (por ex., BUILTIN\Administradores) e a permissão Deny (Negar) foi concedida a um outro grupo do Windows (por ex., BUILTIN \Usuários) no mesmo nível na hierarquia de classes de dispositivos (por ex., Unidades de DVD/CD-ROM). Se um usuário for membro de ambos os grupos (p. ex., Administrador), o que tem precedência?	O usuário tem o acesso negado ao dispositivo. Negar tem precedência a Permitir. O acesso é negado devido ao modo como o Windows determina a permissão efetiva para o dispositivo. Um grupo tem o acesso negado e outro grupo tem o acesso permitido, mas o usuário é membro de ambos os grupos. O usuário tem o acesso negado pois a negação de acesso precede a permissão de acesso. Uma solução provisória é negar o acesso ao grupo de usuários no nível de Unidades de DVD/CD-ROM e permitir o acesso ao grupo de administradores no nível abaixo de Unidades de DVD/CD-ROM. Uma outra solução provisória seria ter grupos do Windows específicos, um para permitir o acesso a DVDs/CDs e outro para negar o acesso a DVDs/CDs. Usuários específicos poderiam então ser adicionados aos grupos apropriados.

Diversos

Impactado por software – Descrição resumida	Detalhes	Solução
Security Manager — Advertência recebida: **The security application can not be installed until the HP Protect Tools Security Manager is installed** (O aplicativo de segurança não pode ser instalado até que o HP Protect Tools Security Manager esteja instalado).	Todos os aplicativos de segurança, como o Embedded Security, o Java Card Security e os dispositivos biométricos são plug-ins expansíveis para a interface do Security Manager. O Security Manager deve ser instalado antes que um plug-in de segurança aprovado pela HP possa ser carregado.	O software Security Manager deve ser instalado antes da instalação de qualquer plug-in de segurança.
Utilitário de atualização de firmware TPM para modelos que contêm TPMs com suporte para Broadcom — A ferramenta fornecida através do web site de suporte da HP relata **ownership required** (propriedade necessária).	Esse é o comportamento esperado do utilitário de firmware do TPM para modelos que contêm TPMs com suporte para Broadcom. A ferramenta de atualização de firmware permite ao usuário atualizar o firmware, com ou sem uma chave de endosso (EK). Quando não há uma chave de endossos, não é preciso autorização para completar a atualização de firmware. Quando há uma chave de endossos, é preciso haver um proprietário TPM, uma vez que o upgrade exige a autorização do proprietário. Depois de atualizar, a plataforma deve ser reiniciada para que o novo firmware entre em vigor. Se o TPM do BIOS for restaurado com os valores de fábrica, a propriedade é removida e a capacidade de atualização de firmware é bloqueada até que a plataforma de software Embedded Security e o assistente de inicialização de usuário tenham sido configurados. **NOTA:** Uma reinicialização é sempre recomendada após a execução de uma atualização de firmware . A versão do firmware não é identificada corretamente após a reinicialização.	1. Reinstale o software Embedded Security. 2. Execute o assistente de configuração de plataforma e usuário. 3. Verifique se o sistema contém o Microsoft .NET Framework 1.1 instalado: a. Clique em **Iniciar**. b. Clique em **Painel de controle**. c. Clique em **Adicionar ou remover programas**. d. Verifique se **Microsoft .NET Framework 1.1** está listado. 4. Verifique a configuração de hardware e software: a. Clique em **Iniciar**. b. Clique em **Todos os programas**. c. Clique em **HP ProtectTools Security Manager (Gerenciador de segurança HP ProtectTools)**. d. Selecione **Embedded Security** no menu em árvore. e. Clique em **Mais detalhes**. O sistema deve ter a seguinte configuração: • Versão de produto = V4.0.1 • Estado de embedded security: estado do chip = ativado, estado de propriedade = inicializado, estado de usuário = inicializado • Informação dos componentes: Versão Spec. TCG = 1.2 • Fornecedor= Broadcom Corporation

Impactado por software – Descrição resumida	Detalhes	Solução
		● Versão de FW = 2.19 (ou posterior) ● Versão de biblioteca de drivers de dispositivo TPM 2.0.0.9 (ou posterior) 5. Se a versão de FW não for 2.18, faça o download e atualize o firmware do TPM. O SoftPaq de firmware do TPM é um download de suporte disponível no site da Web da HP em http://www.hp.com.
HP ProtectTools Security Manager — Intermitente, um erro é exibido ao fechar a interface do Security Manager.	Intermitente (1 em 12 instâncias), um erro é gerado ao utilizar o botão fechar no canto superior direito da tela, para fechar o Security Manager antes que todos os aplicativos de plug-ins tenham sido totalmente carregados.	Isso está relacionado a uma dependência de sincronização no tempo de carregamento de serviços do plug-in, ao fechar e reiniciar o Security Manager. Sendo PTHOST.exe uma carcaça (shell) que comporta outros aplicativos (plug-ins), ela depende da capacidade do plug-in em completar seu tempo de carregamento (serviços). A causa do problema é o ato de fechar a carcaça antes que o plug-in tenha sido completamente carregado. Permita que o Security Manager conclua a mensagem de carregamento de serviços (vista na parte superior da janela do Security Manager) e todos os plug-ins listados na coluna da esquerda. Para evitar falhas, aguarde um tempo razoável para que os plug-ins sejam carregados.
HP ProtectTools — Acesso irrestrito ou privilégios de administrador não-controlados apresentam risco à segurança.	Diversos riscos são possíveis com o acesso irrestrito ao PC cliente, incluindo os seguintes: ● Exclusão da PSD ● Modificação mal-intencionada das configurações do usuário ● Desativação de políticas e funções de segurança	Os administradores são encorajados a seguir as “melhores práticas” para restringir os privilégios de usuários-finais e restringir o acesso de usuários. Usuários não-autorizados não devem possuir privilégios administrativos.
As senhas do BIOS e do OS Embedded Security estão fora de sincronismo.	Se um usuário não validar uma nova senha como sendo a senha do BIOS Embedded Security, esta volta à senha original de segurança integrada através do **f10** BIOS.	Este recurso está funcionando corretamente; as senhas podem ser re-sincronizadas mudando a senha básica de usuário do sistema operacional e autenticando-a no prompt de senha de BIOS Embedded Security.
Apenas um usuário pode acessar o sistema depois que a autenticação pré-inicialização TPM for ativada no BIOS.	O PIN do BIOS do TPM é associado ao primeiro usuário que inicializa a configuração do usuário. Se um computador tiver vários usuários, o primeiro usuário é, essencialmente, o administrador. O primeiro usuário terá que fornecer seu PIN de usuário TPM a outros usuários que o usarão para fazer o login.	Este recurso está funcionando conforme planejado; a HP recomenda que o departamento de TI do cliente siga as boas práticas de segurança para implementar sua solução de segurança e garantir que a senha de administrador do BIOS seja configurada por administradores de TI com proteção de nível de sistema.
O usuário tem que alterar seu PIN para fazer a pré-inicialização do TPM funcionar após uma restauração aos padrões de fábrica.	O usuário tem que alterar seu PIN ou criar um outro usuário para inicializar sua configuração de usuário e fazer a autenticação do BIOS do TPM funcionar após uma restauração. Não há opção para fazer a autenticação do BIOS do TPM funcionar.	Isso foi projetado desta maneira; a redefinição aos padrões de fábrica remove a Chave de usuário básico. O usuário deve alterar seu PIN de usuário ou criar um novo usuário para reinicializar a Chave de usuário básico.

Impactado por software – Descrição resumida	Detalhes	Solução
A opção **Power-on authentication support** (Suporte para autenticação na ativação) não volta ao padrão quando se usa a opção **Reset to Factory Settings** (Restaurar com as configurações de fábrica) do Embedded Security	No utilitário de configuração a opção **Suporte à autenticação na ativação** não foi restaurada com as configurações de fábrica ao utilizar a opção de dispositivo Embedded Security **Restauração das configurações de fábrica**. Por padrão, o **suporte para autenticação na ativação** é definido como **Desativado**.	A opção **Reset to Factory Settings** (Restauração das configurações de fábrica) desativa o Embedded Security Device, que oculta as outras opções do Embedded Security (incluindo **Power-on authentication support** [Suporte para autenticação na ativação]). Entretanto, após a reativação do Embedded Security Device, a opção **Power-on authentication support** permanece ativada. A HP está trabalhando em uma resolução, que será fornecida em ofertas futuras de SoftPaq ROM com base na Web
A Autenticação na inicialização por segurança substitui a senha do BIOS durante a seqüência de inicialização.	A Autenticação na inicialização avisa o usuário para efetuar login no sistema utilizando a senha do TPM, mas, se o usuário pressionar **f10** para acessar o BIOS, ele terá concedido apenas o acesso com direitos de leitura.	Para gravar para o BIOS, o usuário deve digitar a senha do BIOS em vez da senha do TPM na janela Autenticação na inicialização.
O BIOS pergunta por ambas as senhas, antiga e nova, no utilitário Configuração do computador após a senha do proprietário ser alterada.	O BIOS pergunta por ambas as senhas, antiga e nova, no utilitário Configuração do computador após a senha do proprietário ser alterada no software Embedded Security do Windows.	Isso foi projetado desta maneira. Isso deve-se à incapacidade do BIOS de comunicar-se com o TPM, após o sistema operacional estar funcionando, e para verificar a frase secreta do TPM.

Glossário

Administrador. Veja administrador do Windows.

Administrador do Windows. Um usuário com direitos totais para modificar permissões e gerenciar outros usuários.

Arquivo de recuperação de emergência. Área de armazenamento protegida que permite criptografar novamente as chaves de usuário básico, a partir de uma chave de proprietário de plataforma a outra.

Assinante sugerido. Um usuário que é designado pelo proprietário de um documento do Microsoft Word ou do Microsoft Excel para acrescentar uma linha de assinatura ao documento.

Assinatura digital. Dados enviados junto com um arquivo que verificam o remetente do material, e que o arquivo não foi modificado depois de assinado.

Ativação. A tarefa que deve ser concluída antes que qualquer um dos recursos do Drive Encryption possa ser acessado. Para ativar o Drive Encryption, use o assistente de instalação do HP ProtectTools Security Manager. Apenas um administrador pode ativar o Drive Encryption. O processo de ativação consiste na ativação do software, criptografia da unidade, criação de uma conta de usuário e criação do backup inicial da chave de criptografia em um dispositivo de armazenamento removível.

Ativo. Um componente de dados contendo informações ou arquivos pessoais, histórico e dados relacionados à Web, localizado no disco rígido.

ATM (Automatic Technology Manager). Permite que os administradores de rede gerenciem sistemas remotamente no nível do BIOS.

Autenticação. Processo que verifica se um usuário está autorizado a executar uma tarefa, como acessar um computador, modificar configurações de um determinado programa ou visualizar dados protegidos.

Autenticação na inicialização. Recurso de segurança que requer algumas formas de autenticação, como um Java Card, um chip de segurança ou uma senha, quando o computador é ligado.

Autoridade de certificação. Serviço que emite certificados necessários para executar uma infra-estrutura de chave pública.

Biométrica. Categoria de credenciais de autenticação que utilizam um recurso físico, como a impressão digital para identificar um usuário.

Botão Send Security (Segurança de Envio). Um botão de software que é exibido na barra de ferramentas das mensagens de e-mail do Microsoft Outlook. Clicar no botão permite assinar e/ou criptografar uma mensagem de e-mail do Microsoft Outlook.

Botão Sign and Encrypt (Assinar e Criptografar). Um botão de software que é exibido na barra de ferramentas dos aplicativos do Microsoft Office. Clicar no botão permite assinar, criptografar ou remover a criptografia de um documento do Microsoft Office.

Certificado digital. Credenciais eletrônicas que confirmam a identidade de um indivíduo ou empresa, vinculando a identidade do proprietário do certificado digital a um par de chaves eletrônicas que são utilizadas para assinar a informação digital.

Certificado do Privacy Manager. Um certificado digital que exige autenticação toda vez que é usado para operações de criptografia, como assinar e criptografar mensagens de e-mail e documentos do Microsoft Office.

Chat History Viewer (Visualizador do Histórico de Bate-papo). Um componente do Privacy Manager Chat que permite procurar e visualizar sessões de histórico de bate-papo.

Chip de segurança integrada TPM (Trusted Platform Module - Módulo de plataforma confiável) (somente em determinados modelos) É o termo genérico para o chip de segurança integrada HP ProtectTools Embedded Security Chip. Um módulo TPM autentica um computador, e não um usuário, armazenando informações específicas do sistema anfitrião, como chaves de criptografia, certificados digitais e senhas. O módulo TPM minimiza o risco de perda de informações armazenadas no computador por roubo físico ou invasão por hackers externos.

Ciclo de fragmentação. O número de vezes que o algoritmo de fragmentação é executado em cada ativo. Quanto mais alto for o número de ciclos de fragmentação selecionado, maior a segurança do computador.

Comunicação de IM confiável. Uma sessão de comunicação durante a qual mensagens confiáveis são enviadas por um remetente confiável para um contato confiável.

Conta de rede. Conta de usuário ou administrador Windows, seja em um computador local, em um grupo de trabalho ou em um domínio.

Conta de usuário do Windows. Perfil de um indivíduo autorizado a acessar uma rede ou um computador individual.

Contato confiável. Uma pessoa que aceitou um convite para se tornar um contato confiável.

Convite de contato confiável. Um e-mail que é enviado para uma pessoa perguntando se ela deseja se tornar um contato confiável.

Credenciais. Método no qual um usuário comprova sua elegibilidade para determinada tarefa no processo de autenticação.

Criptografia. Prática de codificar e decodificar dados, para que possam ser decodificados apenas por indivíduos específicos.

Criptografia. Procedimento, com a utilização de um algoritmo, empregado na criptografia para converter texto simples em texto cifrado, para evitar que destinatários não-autorizados leiam os dados. Existem diversos tipos de codificação de dados e eles formam a base da segurança de rede. Alguns tipos comuns incluem o padrão de criptografia de dados e criptografia por chave pública.

Descriptografia. Procedimento utilizado na criptografia para converter dados criptografados em texto simples.

Destinatário de contato confiável. Uma pessoa que recebe um convite para tornar-se um contato confiável.

Domínio. Grupo de computadores que fazem parte de uma rede e compartilham de um banco de dados de diretórios comum. Os domínios possuem nomes exclusivos, e cada um possui um conjunto de regras e procedimentos.

DriveLock Recurso de segurança que vincula o disco rígido a um usuário e requer que o usuário digite corretamente a senha do DriveLock quando o computador é inicializado.

DriveLock automático. Recursos de segurança que fazem as senhas de DriveLock serem geradas e protegidas pelo chip TPM de segurança integrada. Quando o usuário é autenticado pelo chip TPM de segurança integrada durante a inicialização, digitando a senha correta de usuário básico de TPM, o BIOS desbloqueia a unidade de disco rígido para o usuário.

EFS (Encryption File System – Sistema de criptografia de arquivo). Sistema que decodifica todos os arquivos e subpastas dentro do diretório selecionado.

Exclusão simples. Exclusão da referência do Windows para um ativo. O conteúdo do ativo permanece no disco rígido até que os dados ocultos sejam sobregravados pela limpeza de espaço livre.

Fragmentação automática. Fragmentação programada que o usuário define no File Sanitizer for HP ProtectTools.

Fragmentação manual. Fragmentação imediata de um ativo ou de ativos selecionados, a qual ignora a programação de fragmentação automática.

Fragmentar. A execução de um algoritmo que oculta os dados contidos em um ativo.

Histórico de bate-papo. Um arquivo criptografado que contém um registro dos dois lados de uma conversa em uma sessão de bate-papo.

HP SpareKey. Cópia de segurança da chave do Drive Encryption.

Identidade. No HP ProtectTools Credential Manager, um grupo de credenciais e configurações que são utilizadas como uma conta ou perfil para um determinado usuário.

Java Card. Um cartão removível que é inserido no computador. Ele contém informações de identificação para o login. O login usando um Java Card na tela de login do Drive Encryption requer que você insira o Java Card e digite seu nome de usuário e o PIN do Java Card.

Limpeza de espaço livre. A gravação segura de dados aleatórios sobre os ativos excluídos para alterar o conteúdo do ativo excluído.

Linha de assinatura. É um local reservado para a exibição visual de uma assinatura digital. Quando um documento é assinado, o nome do assinante e o método de verificação são exibidos. A data de assinatura e o título do assinante também podem ser incluídos.

Lista de contatos confiáveis. Uma listagem de contatos confiáveis.

Mensagem confiável. Uma sessão de comunicação durante a qual mensagens confiáveis são enviadas por um remetente confiável para um contato confiável.

Método de login de segurança. O método usado para efetuar login no computador.

Migração. Uma tarefa que permite gerenciar, restaurar e transferir certificados do Privacy Manager e contatos confiáveis.

Modo de dispositivo SATA. Modo de transferência de dados entre um computador e dispositivos de armazenamento em massa, como unidades de disco rígido e unidades ópticas.

Modo de segurança do BIOS. Configuração do Java Card Security que, quando ativada, exige a utilização de um Java Card e um PIN válido para autenticação do usuário.

Perfil de fragmentação. Um método de apagamento específico e lista de ativos.

Perfil do BIOS. Grupo de definições de configuração do BIOS que podem ser salvas e aplicadas em outras contas.

Provedor de serviços de criptografia (CSP). Prestador ou biblioteca de algoritmos criptográficos que podem ser utilizados em uma interface bem definida para realizar determinadas funções criptográficas.

Public Key Infrastructure - Infra-estrutura de chaves públicas(PKI) Padrão que define as interfaces para criar, utilizar e gerenciar certificados e criptografias chave.

Reinicializar. Processo de reinicialização do computador.

Remetente confiável. Um contato confiável que envia e-mails e documentos do Microsoft Office assinados e/ou criptografados.

Revelar. Uma tarefa que permite ao usuário descriptografar uma ou mais sessões de histórico de bate-papo, exibindo o(s) nome(s) de tela do(s) contato(s) em texto simples e tornando a sessão disponível para exibição.

Segurança estrita. Recurso de segurança do BIOS Configuration que fornece proteção aprimorada para as senhas de inicialização e de administrador e outras formas de autenticação na inicialização.

Selagem para contatos confiáveis. Uma tarefa que acrescenta uma assinatura digital, criptografa o e-mail e o envia depois que você realiza sua autenticação utilizando o método de login de segurança de sua escolha.

Senha de administrador do BIOS. Senha de *configuração* do utilitário de configuração do computador.

Senha de revogação. Uma senha que é criada quando um usuário solicita um certificado digital. Uma senha que é necessária quando o usuário deseja revogar seu certificado digital. Isso garante que só o usuário pode revogar o certificado.

Seqüência de teclas. Uma combinação de teclas específicas que, quando pressionadas, iniciam uma fragmentação automática; por exemplo: ctrl+alt+s.

Serviço de recuperação de chave do Drive Encryption. O Serviço de Recuperação do SafeBoot. Armazena uma cópia da chave de criptografia, permitindo a você acessar o computador caso esqueça sua senha e não tenha acesso a sua chave de backup local. Você deve criar uma conta nesse serviço para configurar o acesso on-line à sua chave de backup.

Single Sign On (Login Único). Recurso que armazena informações de autenticação e permite o uso do Credential Manager para acessar aplicativos de Internet e do Windows que requerem autenticação por senha.

Smart card. Pequena peça de hardware, similares a um cartão de crédito em tamanho e formato, que armazena informações identificáveis sobre o proprietário. Utilizado para autenticar o proprietário de um computador.

Tela de login do Drive Encryption. A tela de login exibida antes do Windows ser iniciado. Os usuários devem inserir seu nome de usuário e a senha do Windows ou o PIN do Java Card. Na maioria das vezes, a inserção da informação correta na tela de login do Drive Encryption permite o acesso direto ao Windows sem precisar efetuar login novamente na tela de login do Windows.

Token. Veja método de login de segurança.

Token USB. Dispositivo de segurança que armazena informações de identificação de um usuário. Como um Java Card ou leitor biométrico, ele é utilizado para autenticar o proprietário de um computador.

Token virtual. Recurso de segurança que funciona de forma muito semelhante a um Java Card e leitor de cartão. O token é salvo no disco rígido do computador ou no registro do Windows. Ao efetuar login com um token virtual, será solicitado um PIN de usuário para completar a autenticação.

TXT. Trusted Execution Technology (Tecnologia de execução confiável).

Unidade pessoal protegida (PSD). Oferece uma área de armazenamento protegida para informações confidenciais.

Usuário. Qualquer pessoa registrada no Drive Encryption. Usuários não-administradores têm direitos limitados no Drive Encryption. Eles podem apenas se registrar (com aprovação do administrador) e efetuar login.

Índice